SEAPORT PROTECTION AGAINST CHEMICAL AND BIOLOGICAL ATTACKS

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
Fulfillment of the requirements for the
Degree

MASTER OF MILITARY ART AND SCIENCE
Strategy

by

Jenifer L. Breaux, MAJ, USA
B.A., Bowling Green State University, Bowling Green, Ohio, 1991
M.A., Texas A&M, Commerce, Texas, 2001

Fort Leavenworth, Kansas
2009

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
04-02-2009	Master's Thesis	Oct 2007 – Feb 2009

4. TITLE AND SUBTITLE
Seaport Protection Against Chemical and Biological Attacks

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Breaux, Jenifer L., Major, U.S. Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
100 Stimson Avenue
Fort Leavenworth, KS 66027

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Since the 9/11 attacks, the DHS has increased security measures at airports. On the other hand, it appears on the surface there has been a disregard of seaport protection. The primary question of this thesis is do United States seaports have adequate preventive measures in place to provide early warning to the public? If there are preventive measures in place, will they assist in preventing chemical and/or biological attacks? The ports of Long Beach and Miami were used for a case analysis. Situated on different coasts, these ports have different population sizes and location but similar economic importance and are large enough that information is readily available. The first section analyzed how federal and local governments provide security, oversight responsibility and the application of current doctrine, plans and legislature. Next, analysis was conducted on the utilization of protection measures and current equipment. Finally, included is the role of the federal government in the protection of maritime domain. The case study suggests that both ports examined have met at least some of the seaport protection requirements as set forth in this thesis. The only area in which both ports failed is in the area of budget allocation, specifically dedicating monetary resources toward equipment research and development.

15. SUBJECT TERMS Homeland Security, Federal Government Seaport Funding, Seaport Protection, Protection and Threat Levels, Chemical Protection Equipment, Biological Protection Equipment, Department of Homeland Security, Port of Miami-Dade, Port of Long Beach, Federal Government Chemcial/Biological Protection Doctrine

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	96	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Jenifer L. Breaux

Thesis Title: Seaport Protection Against Chemical and Biological Attacks

Approved by:

_____, Thesis Committee Chair
Richard E. Berkebile, M.S.

_____, Member
Jack D. Kem, Ph.D.

_____, Member
Robert Walz, M.A.

Accepted this 4th day of February 2009 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency.

ABSTRACT

SEAPORT PROTECTION AGAINST CHEMICAL AND BIOLOGICAL ATTACKS, by MAJ Jenifer Breaux, 96 pages

Since the 9/11 attacks, the DHS has increased security measures at airports. On the other hand, it appears on the surface there has been a disregard of seaport protection. The primary question of this thesis is do United States seaports have adequate preventive measures in place to provide early warning to the public? If there are preventive measures in place, will they assist in preventing chemical and/or biological attacks? The ports of Long Beach and Miami were used for a case analysis. Situated on different coasts, these ports have different population sizes and location but similar economic importance and are large enough that information is readily available. The first section analyzed how federal and local governments provide security, oversight responsibility and the application of current doctrine, plans and legislature. Next, analysis was conducted on the utilization of protection measures and current equipment. Finally, included is the role of the federal government in the protection of maritime domain. The case study suggests that both ports examined have met at least some of the seaport protection requirements as set forth in this thesis. The only area in which both ports failed is in the area of budget allocation, specifically dedicating monetary resources toward equipment research and development

TABLE OF CONTENTS

Page

ACRONYMS

AIS	Automatic Identification System
AMS	Area Maritime Security Plan
BAWS	BioAttack Early Warning System
CBP	Customs and Border Protection
CBRNE	Chemical Biological Radiological Nuclear Effects
CIA	Central Intelligence Agency
COP	Common Operating Picture
CSI	Container Security Initiative
C-TPAT	Customs-Trade Partnership Against Terrorism
CW/BW	Chemical Weapons/Biological Weapons
DHS	Department of Homeland Security
DOD	Department of Defense
DoJ	Department of Justice
DOS	Department of State
EOC	Emergency Operations Center
FBI	Federal Bureau of Investigation
FMTA	Federal Maritime Transportation Act
GAO	Government Accountability Office
GPS	Global Positioning Systems
GSM	Global System for Mobiles
HSOC	Homeland Security Operations Center
HSPD	Homeland Security Presidential Directive

ISAC	Information Sharing and Analysis Centers
JFO	Joint Field Office
LTTE	Liberation Tigers of Tamil
MDA	Maritime Domain Awareness
MTSA	Maritime Transportation Security Act
MIRP	Maritime Infrastructure Recovery Plan
NIPP	National Infrastructure Protection Plan
NMSP	National Maritime Security Plan
NOC	National Operations Center
NORTHCOM	Northern Command
NRF	National Response Framework
NSA	National Security Advisor
NSPD	National Security Presidential Directive
NSMS	National Strategy for Maritime Security
NTC	National Targeting Center
R&D	Research and Development
SAFE Port Act	Security and Accountability for Every Port Act
TSA	Transportation Security Administration
TSSP	Transportation Sector Specific Plan
TWIC	Transportation Workers Identification Card
US	United States
USCG	US Coast Guard
WMD/E	Weapons of Mass Destruction/Effect

ILLUSTRATIONS

Page

TABLES

Page

CHAPTER 1

SEAPORT SECURITY WTIHIN THE MARITIME STRATEGY

Introduction

During a 2002 workshop organized by the Swedish Minister of Foreign Affairs, RAND Europe presented several papers, one of which discussed terrorists' actions. While presenting the likelihood of enemy attacks on shipping containers, they argued, "The container supply chain does not pose a likely target, however some terrorist groups like the Liberation Tigers of Tamil (LTTE) have been known to attack maritime targets. From their past actions, it would not be a drastic turn to use container transport as a means of distributing terror" (RAND 2003). The purpose of this thesis is to examine maritime security, focusing specifically on seaports and their preventive measures against chemical weapons/biological weapons (CW/BW). A heightened awareness occurred after four coordinated attacks occurred on 9/11 and with this awareness, protection and security measures were implemented. New efforts to prevent future coordinated attacks or any attack on United States soil have increased significantly. Implementation of security measures for airports as well as land ports of entry from both Canada and Mexico occurred.

Our way of life requires that cargo entering the United States remains secure. Mass hysteria, environmental pollution, and large debt incurred by a massive clean up for a CW/BW attack are minor compared to the other effects such as on domestic and global economies, or our way of life. It is vital to not only the survival of our economy, but also the survival of the United States population that we have proactive measures and

procedures in place to address and prevent terrorist attacks on United States seaports. With the common practice of just-in-time inventories as well as supplies of food that are largely imported, the effects of disruption to the supply chain will take weeks and possibly months to untangle if contamination of seaports forces their closure following such attacks.

Problem Identified

Since the 9/11 attacks, the DHS has increased security measures at airports, implemented more stringent restrictions as to who can enter the country, increased guidelines for traveling abroad to include to and from Canada and Mexico, added limitations to those vacationing on cruise ships and implemented new passports which contain microchips. Security measures at airports are continuously scrutinized and airports receive incessant press coverage. Tighter restrictions occur constantly and now include the practical elimination of carrying liquids onboard aircraft. However, it appears on the surface there is a disregard of the protection of seaports to include early warning and response protocols. There are millions of pounds of cargo entering the United States every day with ninety percent arriving through its seaports. Inspection of approximately one percent of this cargo occurred in 2001 but increased to five percent by 2005. The United States National Strategy for Maritime Security (NSMS), as well as articles in various publications, recognizes that the maritime domain is a viable avenue of approach for terrorists. These documents specifically mention that non-state actors are observing how we conduct daily operations and security procedures. They are searching for any

gaps in security procedures in order to exploit these gaps and cause havoc. Their willingness to use weapons of mass destruction remains a strategic concern.

Research Question

The primary question that this thesis will focus on is do United States seaports have adequate preventive measures in place to provide early warning to the public? The follow up question to this is if there are preventive measures in place, will they assist in preventing chemical and/or biological attacks? A National Maritime Strategy does exist, however it appears on the surface that seaports do not receive the same emphasis level as other ports of entry. Monetary funding, security analysis, intelligence collection, and awareness appear nonexistent. With inspection of less than five percent of cargo containers, the United States has left itself vulnerable. Any of its enemies has a unique opportunity to weaken the United States by using seaports and shipping containers as a means to attack.

Secondary Questions

From this primary question, there are secondary questions that surface and are worthy of exploring. The first secondary question is how do we currently provide security of our ports? A needs analysis was conducted of the current port security policies and regulations in place as well as doctrine and responsibility for oversight of the security. There are roles and responsibilities of the private sector, emergency services, as well as the local, state, and federal government. Defined areas of responsibility between all these agencies are required for a cohesive and synchronized protection effort.

In addition to how we currently provide port security, another question that arises is what are the current protection measures? If defined protection measures exist, are they tied to the national threat levels? If they are not, do they need to be, are they confused with the national threat levels, and does the general public need to be aware of these threat levels? If the answer is yes, then perhaps any threat level that exists or will exist will need to be tied to national threat levels. For protection of strategic assets, allocation of resources is warranted. However, it is important to understand operational and tactical equipment currently used to protect seaports in order to allocate appropriate levels of funding. Each seaport has its nuances and challenges and, therefore, there is no requirement for equipment to be standardized. More importantly, the focus for this paper is at the strategic level. Resource allocation and requirements will focus on necessary budgets and new programs needed.

In addition to current port security measures and current protection measures, the final secondary question is what role does the Federal Government, more specifically the DHS, play in seaport security? Details of how the DHS operates and their role must include not only funding and distribution of funds but also who gathers and conducts analysis of the current threat and dissemination of information to those levels of government that need the information and can act on reliable and credible information. Information sharing with private sectors that have a role in the security of our national ports should also be defined.

Assumptions

In order to facilitate analysis and discussion of our national security and protection of our seaports there are two applicable assumptions which must be considered. The first assumption is that the enemy is currently researching and testing ways to attack the United States through its ports and more specifically with containers. Another assumption is that the enemy is constantly conducting reconnaissance of our ports, port security, and our response mechanisms and annotating predictable techniques and practices.

Key Terms

Below are the key terms critical to understanding before proceeding. Additional terms are contained within the glossary.

Critical Infrastructure. Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (DHS 2007).

Emergency. Any incident(s) whether natural or manmade, that requires responsive action to protect life or property; any occasion or instance for which Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States (DHS 2007).

Enemy. Any organization to include nation-states, terrorists, transnational criminals and pirates that views the United States as an adversary and is not limited to

nation-states, terrorists, and transnational criminals and pirates, dispersed terrorist networks (DHS 2007).

Local Government. A county, municipality, city, town, township, local public authority, council of governments, regional or interstate government entity, an Indian tribe or authorized tribal entity (DHS 2007).

Maritime Domain. All areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean or other navigable waterways, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances (DHS 2007).

Stakeholders. Federal agencies to include executive agencies departments and government corporations, local agencies (DHS 2007).

Weapons of Mass Destruction/Effect (WMD/E). For this thesis describes chemical or biological agents or weapons and effects – terrorist attack to achieve mass effect in terms of mass casualties, destruction of critical infrastructure, economic losses, and disruption of daily life nationwide (DHS 2007).

Limitations and Delimitations

Maritime security is a large area and can include the ports themselves, the coastline, and the waterways approaching the United States. There are limitations and delimitations for this thesis. There are only two limitations; only open source and unclassified documents were used. Additionally, information cutoff date of the research was December 15, 2008. While there are two limitations, there are several delimitations, which are closely related to this thesis. The first delimitation is that this thesis will not include radiological or nuclear attacks or affects as analysis of these types of weapons

systems, doctrine, and response to attacks is different from CW/BW attacks. For radiological weapons, soil type, inside dose rate, outside dose rate, detection equipment and decontamination procedures and chemicals are different. Although CW/BW agents have different chemical structures, they do have similarities to include how the atmospheric conditions affect agents, response to an attack, and similar decontamination equipment. Additionally, research will not analyze use of seaports as entry points to move Chemical Biological Radiological Nuclear Effects (CBRNE) to interior United States cities. This thesis will only focus on the seaports themselves and will not include waterways or the coastline itself. This thesis will not consider any inner coastal ports, navigable rivers, or inland waterways, nor will it look at over-the-road delivery of containers within the continental United States, Alaska or Hawaii. This thesis will only consider external delivery of containers. Additionally, research will not include attempts or successful cyber attacks on significant information systems, which are critical to maritime operations. The final delimitation is that this thesis will only look at security of ports themselves and therefore will not explore or analyze security of maritime domain from the shoreline outward.

Significance of Study

Determining the scope of the thesis was important in order to understand what will be included in the research and final publication of this thesis. This research and conclusions are important for several reasons. The first is that security vulnerabilities exist including the fact that land is easily accessible by water and the coastal border is porous, as it is not continuously patrolled due to the extensive coastline but also due to

assets maintained. Assets include a small Coast Guard fleet, and although its annual budget has increased over recent years, that is still not large enough to patrol the vast area. The limited number of customs agents and quantity of container detection equipment are vulnerabilities that a terrorist organization can exploit and launch an attack. In the supply chain screening and credentialing of cargo ships is weak. This presents another weakness within our system that an enemy can use against America. After conducting analysis, identifying weaknesses and conclusions, government agencies as well as the private sector could use this information to facilitate a coordinated effort to rectify gaps in the current strategy. Another significant factor is that data and suggested protocols gathered during research and analysis will create domain awareness to identify early indicators and warnings. This can enable appropriate response, thus creating public awareness and reducing mass hysteria. Findings from this research and creating awareness have the potential to influence key legislation affecting national commerce. Increased port security and information sharing across all spectrums of responsibility has the potential to prevent port closure by increased awareness and to ensure continued supply of all logistics such as food, fuel, and other imports and commerce to the entire country.

Summary and Conclusions

Security of our seaports has increased, albeit at significantly reduced funding, by means of additional legislation as well as time and effort spent on creating feasible plans. Is United States maritime security weak? Although port security legislation exists, an analysis will examine if it does enough to protect the United States citizens and its supply

chain from terrorist attacks. Shipping containers and delivery of them is an avenue the enemy can use against America to launch CW/BW attacks against its seaports. Coordination between government officials at all levels and the private sector are vital to protecting the infrastructure. Legislation, funding, intelligence gathering and sharing, and doctrine are all key aspects in determining if United States seaports have adequate protection measures in place to provide early warning and prevent CW/BW attacks.

This chapter has established the thesis statement and secondary questions. Key terms and the scope will aid in understanding further chapters and discussion. A review of literature from a variety of resources, journals, case studies, interviews, and reading our national strategic documents will be presented in the next chapter. The United States government policies and current legislation are the foundation of the literature review. A review of two ports within the United States will uncover local governmental and private sector security responsibilities.

CHAPTER 2

REVIEW OF LITERATURE

Introduction

In recent years, port security has received a lot of attention. Plans were discussed and created to protect our ports, specifically our airports. Protection of seaports appears to have lagged behind. As stated in chapter 1, the purpose of this thesis is to examine maritime security, focusing specifically on seaports and their preventive measures against CW/BW. A literature review was conducted to disclose the different thoughts on the subject from various writers, national strategies, arguments, and examples of preventive measures.

There is an extensive amount of national strategies written by numerous federal agencies, or in collaborations with outside think tanks, as well as a variety of articles, books, and journals written by authors with varying opinions on the subject. This chapter will focus on providing information on what currently exists on the protection of our seaports, national policies, federal plans, and previous policies. There are opinions written which state that the federal, state, and local governments are on track with planning, equipping, and communicating within every level of government. However, there are also differing opinions that governments at all levels are lagging behind in planning, resourcing and implementing preventive and protection measures leaving the United States vulnerable to future attacks. Finally, the importance of this study is demonstrated at the end of the chapter.

Existing Publications

Current National Policies and Plans

Terrorists have indicated a strong desire to use WMD (TWH 2002). Because of this threat, it is strategically imperative that polices and plans exist. Some of the documents created are within several years of post-9/11 and provide a representation of identifying that there is a threat as well as the need for solutions. Additionally, national strategies and incident response documents were created several years after the initial documents. These resources provide a background and insight into the thought processes of those working within the federal government and its agencies. They lay the foundation and guidelines by which all public and private sectors are required to operate. The National Security Presidential Directive (NSPD)-41: Maritime Security Policy and Homeland Security Presidential Directive (HSPD)-13 entitled Maritime Security Policy established United States policy and guidelines with the focus on maritime security. The directives expressed the importance of cooperation at all levels of government, in the public sector, and among the international community.

Strategies and Plans

As the NSMS states that although government is working with international partners on doctrine for the prevention of attacks and creating domain awareness within shipping lanes, appropriate doctrine and responses must exist in the event that early identification fails to prevent attack on seaports (NSMS 2005). It is with this statement that this paper will lay out the need for various policies and plans. This strategy sets the guidelines in regards to communication, coordinating with the international community,

and conveys that a plan is needed. The NSMS also recognizes the myriad challenges to achieving its goals to include gaining the trust of international partners. This strategy identifies that incorporating operations and measures along with deterrent and interdiction capabilities will be the most effective in preventing a maritime incident. There are several other plans that lay out the foundation as illustrated in figure 1.

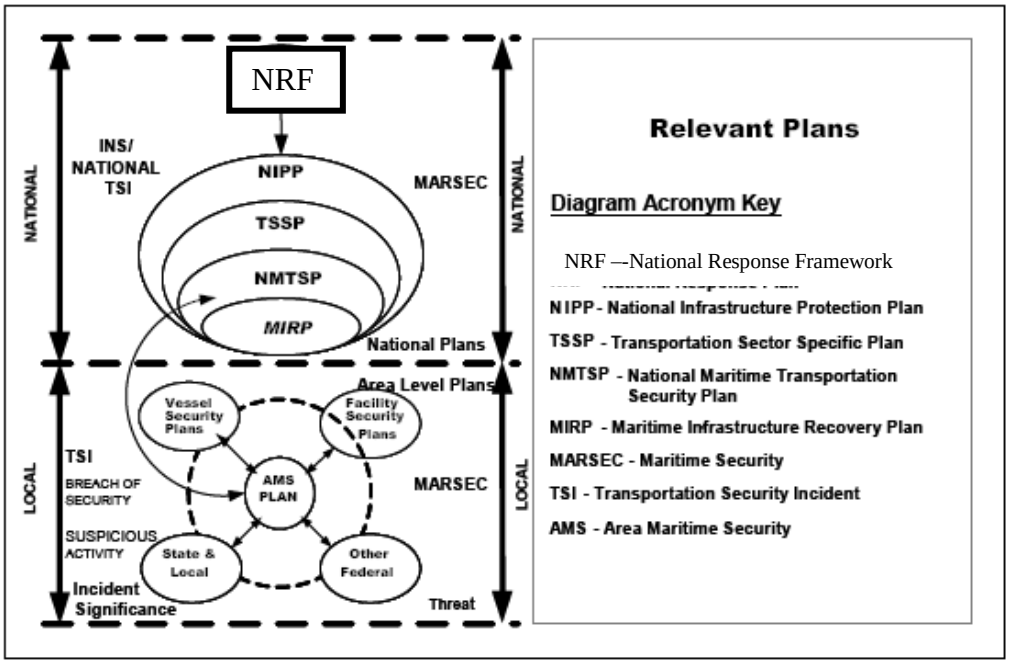

Figure 1. National Strategic Documents Diagram
Source: The White House, *Maritime Infrastructure Recovery Plan for the National Strategy for Maritime Security* (Washington, DC: Government Printing Office, 2005), 24.

In addition to the NSMS, there are several other plans that lay the foundation for how the various federal agencies and departments will plan and execute incident prevention and response. Several plans focus on instituting protection with the first one being the National Infrastructure Protection Plan (NIPP). The NIPP specifies how

coordination and communication among key players will occur in order to protect maritime infrastructure. The National Maritime Security Plan (NMSP) encompasses domestic maritime security and addresses key players at the federal, state, and local levels of government and their responsibilities.

In addition to protection, there are numerous plans that focus on recovery and incident management. The National Response Framework (NRF) establishes the structure for incident management, and restoration of key infrastructure. It is the key plan from which other plans are derived. The Area Maritime Security Plan (AMS) includes guidance for the recovery of systems, ports, and waterways in the event an incident occurs. The Transportation Sector Specific Plan (TSSP) addresses restoring transportation service, infrastructure, and public security. Finally, the Maritime Infrastructure Recovery Plan (MIRP) provides guidelines for recovery management, details responsibilities of the government and doctrine relationships. Below is a pictorial representation of the pertinent plans detailed above and their relationship to the various levels of government.

Finally, the National Plan to Achieve Maritime Domain Awareness, created in 2005, states that the basis for effective prevention is knowledge sharing at all levels of government and private sectors agencies. It also discusses standoff detection capabilities, which will be explored in chapter 4 of this thesis.

Key Legislation

As figure 1 above illustrates, a variety of plans exist. Linkage of plans and integration with each other at all levels of government achieves a unity of effort. The

same applies to legislation. To achieve unity of effort and operational effectiveness governments at all levels must have the capability and authority to operate mutually supporting and complementary roles against the spectrum of expected security threats (TWH 2005). In order to achieve a unity of effort, the first act that was established was The Maritime Transportation Security Act of 2002 (MTSA) which amended the Merchant Marine Act of 1936. The intent of this act is protection, requiring the federal government to address vulnerabilities, and it specifies requirements for international ships. MTSA also includes the Maritime Improvement Policy Act of 2002 and the Coast Guard Personnel and Maritime Safety Act of 2002, both of which address personnel management, miscellaneous certificates of documentation for maritime safety such as spills and modification to reporting requirements.

Another key document is the Security and Accountability for Every Port Act (SAFE Port Act) of 2006, which focused on port security and outlined key programs to include cargo security, screening and credentialing as well as requiring the DHS to provide measurable goals and mechanisms. This act also requires DHS to develop response plans, be the coordinating body for intelligence sharing, and assigns them overall responsibility for coordination with all key agencies.

Both the MTSA and SAFE Port Act focused on protection and measurable goals. Another key piece of legislation is the Customs-Trade Partnership Against Terrorism (C-TPAT). It focuses on the security of the supply chain in regards to terrorism, and designated the Customs and Border Protection Agency as the lead for implementation. C-TPAT stresses the importance of public and private relationships and the coordination

and communication with each other. C-TPAT's goal is to streamline inspections, reduce delays in processing containers, and implement incentives to those that complied within specified timelines.

Although not as an important as MTSA or the SAFE Port Act, the Enhanced Border Security and Visa Entry Reform Act of 2002 is relevant to this thesis. This act authorizes funding for hiring and training personnel, information sharing, electronic visa, and preclearance programs for aliens. Another important item is that law enforcement and intelligence agencies are directed to share intelligence and information as well as utilize a compatible communication systems and technology.

Outside Government Authors

Think tanks, such as the Heritage Foundation and others, provide an outside look at maritime issues and proposed solutions to those challenges that America faces. Additionally books, articles, and journals by independent works are readily available. Upon reading a variety of available resources to include numerous articles, national strategic documents and several papers written by those who are members of the Heritage Foundation, Brookings Institute and Rand Corporation, there is one item that all agree on and that is the need to protect our sea ports. While national strategic documents lay out guidelines on how to accomplish this, those working outside governmental organizations disagree that significant progress and procedures have been fully implemented. All agree that there is a future viable threat from anyone wishing harm to the United States and its interests, but do not specify what or from where the threat is occurring. Many authors, such as James Carafano and Alane Kochems, believe that the government needs to

increase its resources and address the gap between current protection measures and the required measures. Additionally, many publications to include the Heritage Foundation are sympathetic and state realistically that in order to prevent economic impacts not only for our country but for the international community as well, one hundred percent of all containers cannot be inspected. The focus should be on prevention and stringent regulations regarding the registration of ships from reliable countries.

In a recent news story, *international cnn.com* reported that all the regulatory guidance and legislation enacted still had gaps, which terrorists could use to disrupt America's way of life. The SAFE Port Act and C-TPAT set the guidelines for those in the supply chain to follow. However private actors are allowed to self report security information, auditing is not required by third-party agencies and there is no follow up in place to ensure users are within the guidelines established. CNN cites a Government Accountability Office (GAO) report encouraging steps be taken to ensure compliance with guidelines and policies established (CNN 2008). A RAND Report written five years earlier declared the same thing, there is a need for an integrated assessment of global threats, risks, and existing and potential security measures (RAND 2003). The report also stated that a detailed examination of strategies, testing for feasibility of plans and execution of them is required (RAND 2003).

A variety of agencies agree that integrated assessment and testing on a continual basis is required (NSMS 2005). Additionally, in order to accomplish successful protection, agencies need interagency communication and cooperation. A GAO report released in 2002 stated, no effective mechanism exists to coordinate and disseminate

threat information at the seaports (GAO 2002). In a separate report in 2005 entitled *Container Security*, GAO observed that although information sharing had improved further modifications are required (GAO 2005). The Heritage Foundation agreed that integration and cooperation by all stakeholders are critical in the success of protecting American seaports. The article *Making the Sea Safer* focused on domestic and international relationships and cooperation to include sharing responsibility and resources. Partnerships between various departments within the government to include Homeland Security, Defense and State were critical from the onset of all planning to ensure all stakeholders at all levels of government, private sector and international community across all spectrum of operations were synchronized. Finally, Daniel Byman with the Brookings Institute stated in 2007 that the FBI's emphasis concerning intelligence gathering and sharing is still lacking (Brookings Institute 2007). The FBI does not produce regular reports therefore other government agencies do not have current situational awareness and threat assessments. This lack of information prevents local government agencies from making decisive policies and plans to ensure seaport protection and attack prevention.

Agreement varies as to who should be responsible, but the majority of resources read agree that an increased allocation of funding is required if seaport protection and prevention of attacks is to be successful (NRF 2008). A recent Brookings Institute report stated, in recent years, the government has greatly increased its spending to protect physical infrastructure, however most efforts have focused on protecting federal assets, primarily Department of Defense (DOD) and Department of State (DOS) (Brookings

Institute 2008). A local paper in Long Beach, CA states that although the federal government has allocated funding, it covers the bare minimum for upgrading systems and security versus implementing proactive measures (Grunion Gazette 2006). In a report written by a member of the Center for American Progress, funding allocated does not match the programs which need implementation, resource allocation is not analyzed and distributed to those ports who are in a higher need and the Port Security Grant Program does not receive its due importance (Center for American Progress 2005).

Contradictions to Popular Opinion

Although government policies, plans, and legislation set the tone and guidance for creating and implementing the vision of a variety of departments as well as the executive branch, there are contradictions written into its own documents. The MIRP states, with over 2,100 possible threat scenarios in hundreds of ports, the variable affecting maritime transportation system recovery is too myriad to provide detailed procedures (TWH 2007). It is the responsibility of all levels of government to create feasible and suitable plans. Government, in conjunction with the private sector and response organizations, should continuously exercise plans and continuously improve them. The MIRP appears to justify generic plans, overarching ideas and excusing themselves from detailed planning. In a RAND technical report, it stated that C-TPAT is a voluntary program and although oversight rests with various government agencies located at the port, it assigns no responsibility to any level of government. Responsibility lies strictly with the stakeholders in the supply chain. Domestic Outreach is part of NSPD-41 and HSPD-13 stating that the interests of both government and private sectors are considered. C-TPAT

contradicts this by making participation voluntary while NMSP assigns responsibility to government leaders and organizations. A program cannot be voluntary while at the same time stating the government will write and execute plans to ensure protection of United States seaports against enemy attack. It further goes on to say that initiatives focus on the priority of prevention and deterrence; however few [government] initiatives have focus on improving fault tolerance or resilience of the system (RAND 2004).

There are some contradictions within a few government plans and a variety of authors point out that self-reporting and regulation is unacceptable. Another contradiction is communications. In regards to standard communication equipment and information sharing, there is room for improvement as a variety of think tanks point out. However, a fact sheet released in 2005 on the DHS announced a security and prosperity agreement among the United States, Canada, and Mexico. It presented unified information sharing and incident management response for those incidents that affect the border areas. With this agreement, communication systems that are actually able to communicate with each other will become the standard. In order to evaluate response protocols, joint exercises were conducted.

Although many authors take a doomsday approach and have a litany of items that the government has failed to produce in ensuring our shores are protected, The Council for Excellence in Government conducted a survey to measure the public readiness as well as the public's opinion on their local government's readiness to protect the city. The survey results varied by location, but almost forty percent stated that their community had a disaster plan and over forty percent had knowledge of the local emergency plan (The

Council for Excellence in Government 2006). The study goes on to report that one of the seven steps recommended to take when preparing for disaster was taking a first aid class which sixty-three percent of Americans had achieved (The Council for Excellence in Government 2006).

Summary

This chapter established the federal government's strategies and plans thus laying a foundation for analysis. A variety of legislation exists today to provide guidelines and the framework for various stakeholders to operate within. Numerous authors have studied, analyzed, and written about maritime security. Many agree that the government has numerous gaps in its protection and prevention plans. These gaps include intelligence gathering and sharing, communication at all levels of government and communication with key stakeholders such as the private sector and the international community. Other gaps include funding and providing monetary resources for the programs that are in place along with determining a priority for which to distribute funds. Still lacking are self-reporting and third-party auditors to serve as honest brokers in evaluating against standards for which all stakeholders should be accountable.

Although there are many experts who state that there are numerous gaps in maritime security, many authors feel that progress continues and the maritime community is on track towards protecting the maritime domain. In fact, in surveys conducted, almost half of the public understands that maritime security plans exist and are familiar with them (The Council for Excellence in Government 2006). Some would argue that the federal government's plans create a one-over-the world approach, but the government

seemingly understands that each port must work autonomously as no two ports are the same. Indications are government understands reality and that emplacing numerous requirements such as inspecting all containers is unrealistic, is cost prohibitive and the supply chain would slow down thus effecting the economy.

This thesis will provide an understanding of the guidelines, policies and plans enacted by the federal government, provide an overview of other experts in the field and present different schools of thought. Additionally, a case study between two different United States ports is included. An analysis between the ports, how they have applied doctrine and legislation is included and allows comparison of two representative cases. Furthermore, no document exits which provides an analysis between the policies and plans set forth by the government and what is actually occurring in the various cities.

The next chapter is a review of the research methodology utilized to obtain information about the security of our seaports. Additionally, criteria used to develop the feasibility and suitability of each resource and analysis conducted of each is included.

CHAPTER 3

RESEARCH METHODOLOGY

Introduction

The previous chapter established a thorough literature review, which included a wide range of books, articles, think tanks' publications, national documents, GAO reviews, and legislation. The purpose of this thesis is to examine maritime security, focusing specifically on seaports and their preventive measures against CW/BW. The first step utilized during the research process was to start with National Strategy Documents and topical websites. Research threads surfaced from these basic documents. Obtaining an overview of current policies and protection measures occurred. Exploration and development of these threads continued with the review of news magazines, newspapers, and other topical websites to obtain current information in the area of port security and chemical/biological threat. Finally, creation of a research plan matrix focused data collection on pertinent information. This chapter is organized into two different sections with the first presenting the background. This establishes the steps taken to obtain information to address the primary question of this thesis. The second part of this chapter focuses on the evaluation criteria used throughout the research process and provides details of the chosen method of research.

Background

The basic research methodology is to examine two case studies of two ports, one on each coast. Obtaining an overview from National Security Strategies, plans and other documents is critical before a case study could be conducted. These provide strategic

guidance from which it is possible to determine evaluation criteria. The two ports selected are Port of Miami-Dade located in Florida on the east coast and the Long Beach Port in California located on the west coast of the United States. These ports were selected because they are located on opposite coasts and are large enough that research and documentation exists. Because of their economic importance and the relatively sizeable private and governmental work forces, Long Beach and Miami should be considered "best case" studies. A comprehensive review of each port in regards to its doctrine, strategic plans, and policies will be explored and compared with each other. Additionally, analysis of its interpretation and compliance with national documents will be included. Port Commission organizations exist for both. Exploring port relationships with various activities to include NGOs, emergency response organizations, the private sector, and local communities is critical in understanding responsibility for oversight. With this information on each port, it can be linked back to the vision and guidance in the national documents and analyzes compliance with each.

Evaluation Criteria

It is possible to evaluate the two ports utilized in the case study based on numerous criteria; however, this thesis focuses on three overarching criteria in order to focus on the primary and secondary research questions. The three overarching criteria used are doctrine and interagency relationships, application of doctrine and plans and funding. Each criterion remains focused on the primary thesis question. The primary question that this thesis will focus on is do United States seaports have adequate preventive measures in place to provide early warning to the public? If there are

preventive measures in place, will they assist in preventing chemical and/or biological attacks?

Doctrine and Interagency Relationships

1. Local plans. Local governments have written plans, they are reviewed periodically and updates are made. Local governments have established and follow processes for continuous improvement.

2. Partnerships. Local governments established partnerships with the private sector. Established plans are inclusive of all private sector partnerships, local response agencies and other government agencies. Plans assign responsibility to each actor, establish a system of checks and balances and communication protocols.

3. Information sharing. Execution of 360-degree information sharing occurs at all levels: top to bottom, bottom to top, with neighbors, the private sector, other partnerships and with response agencies. Information sharing includes providing current and timely enemy information.

Application of Doctrine and Plans

1. Application of Doctrine. Local plans incorporate strategic guidance set forth in national plans and legislation. Local governments comply with national objectives.

2. Exercises. Local governments conduct a variety of exercises. Plans include how often, types of exercises, with whom to include local partnerships and other counties, other organizations such as FEMA, Hospitals, and colleges. DHS coordinates National Exercise program, requires Federal agencies to participate, and incorporates exercises at state and local level.

3. Training. Local plans include a training program. They account for training at all levels. An established training program should include internal training for those within the local government as well as an external training program designed for partners and outside agencies.

Funding

1. Grants. There are numerous grants available. Receiving grants increases disposable income giving the local government more flexibility in the execution of its spending. This criterion include how many grants each year the port applies for and how many they receive.

2. Budget allocation – Research and Development (R&D). Due to the numerous gaps identified in chapter 2, it is important that local governments continue research and development in order to increase its capability in detection and prevention of CW/BW attacks. This criterion focuses on local governments continued quest for self-improvement by allocating funds necessary for R&D.

3. Budget allocation – Infrastructure. Along with R&D, it is necessary for continued infrastructure improvement. Local government allocation on infrastructure is necessary to continue to reinforce and upgrade to the maximum extent possible to fortify its port in the event that prevention of CW/BW attack was not successful.

A comprehensive chart summarizes the analysis of both ports and facilitates a side-by-side comparison. This thesis uses a qualitative analysis approach and a trichotomous rating - completely, partial or not at all to analyze the two ports. In chapter 4, table 1 will be populated. There are two threats to the validity of port comparison.

The first is that the information is highly subjective based on my research and conclusions. Secondly, only two ports were utilized during this study. Due to the paucity of sources and the time available for research, the small number of cases were a necessary evil.

Table 1. Blank Case Study Comparison Chart of the Ports of Long Beach and Miami-Dade

Evaluation Criteria	Port of Long Beach	Port of Miami-Dade
Doctrine and Interagency Relationships		
Local plans written		
Local plans follow strategic guidance		
Local government establishes partnerships with private sectors		
Communications systems in place		
Application of Doctrine and Plans		
Applied federal documents within local plans		
Applied legislation within local plans		
Exercises conducted with local public and private sectors		
Exercises compliant with federal guidance		
Training conducted		
Funding		
Applied for federal grants		
Budget allocation – R&D		
Budget allocation – Infrastructure Improvements		

Summary

This chapter established the background of the national strategic documents as the foundation for creating evaluation criteria. The evaluation criteria include three overarching categories: doctrine and interagency relationships, application of doctrine

and plans and utilization of funds. Under each evaluation criterion, the thesis will drill down even further to ensure a detailed understanding of the case study exists. The detailed criteria include the creation of local plans, partnerships with private sector organizations, and sharing of information at all levels. Additional criteria are the application of doctrine to ensure it is compliant with national objectives, conducting exercises, and training. The final three detailed criteria include funding a variety of projects and requesting grants from the federal government. Definitions for each criterion were established. These definitions facilitate analysis of the two ports identified for the case study.

Answers to the primary and secondary research questions are presented in chapter 4 through a qualitative comparison of the two ports.

CHAPTER 4

RESEARCH ANALYSIS

Introduction

The previous chapter provided information on the research methodology used during the research process. An initial review started with the National Strategy documents and topical websites. Other sources included magazines, books and non-government websites and think tanks facilitating an understanding of various ideas, plans, policies, and protection plans. Criteria were established along with the creation of a research matrix. The purpose of this thesis is to examine maritime security, focusing specifically on seaports and their preventive measures against CW/BW. This chapter has three parts, facilitating the analysis of the material and information gathered during the previous chapters. First, this chapter answers the primary question and secondary questions established in chapter 1. Within each of these areas are answers to tertiary questions, which serve to expand on the secondary questions. Second, an analysis is presented of two ports using the information revealed within the primary and secondary questions. Finally, utilization of a research matrix provides a comparison of two ports utilizing the criteria established during chapter 3.

Primary Research Question

The primary question and focus for this thesis is do United States seaports have adequate preventive measures in place to provide early warning to the public? If there are preventive measures in place, will they assist in preventing chemical and/or biological

attacks? In an attempt to answer the primary question, secondary and tertiary questions evolved. Provided are answers and analysis to these questions throughout this chapter.

Secondary Research Questions

There is a need for full cooperation and intelligence sharing among all levels of government, private and public sectors and should be integrated and coordinated thus ensuring a succinct and seamless effort in protecting our seaports (TWH 2005). Secondary and tertiary questions were established in order to answer the primary research question. These questions explore the details in order to understand the security of our nation's ports and facilitate answering the primary research question. This section answers three secondary questions and eight tertiary questions.

How Do We Provide Security?

The first secondary question explored is how do we provide security? To understand this, one must understand the relationship between the local governments and a variety of agencies within the local area. The exploration of relationships continues by looking at who is responsible for oversight within the security realm. Finally, presented is an examination of what current doctrine exists.

Relationship Between Local Government and Outside Agencies

All levels of government as well as the private sector are responsible for part of the maritime security and must provide resources equal to the portion of responsibility. The MIRP provides procedures for recovery management. It provides guidelines, procedures, and process for all levels of government on how to set priorities.

The MIRP provides guidance, however the Homeland Security Operations Center (HSOC) serves as the nerve center for operations. The HSOC is the national center for domestic incident management. The HSOC operates under the Secretary of DHS and directs coordination amongst all local and emergency agencies. The HSOC shares real-time situational awareness and a common operating picture to all agencies involved in incident management and recovery. HSOC must conduct network centric operations so that all agencies can get the right information at the right time and place. Network centric operations for this analysis means linking knowledgeable entities together so each can share information and act in a coordinated manner (Heritage Foundation 2005). All partners must share responsibility for the establishment of maritime security. Each must provide the resources equal with its responsibility (Heritage Foundation 2005).

Although the HSOC is the national operations center, governments at all levels will be successful by encouraging and creating partnerships with the private sector. The supply chain, infrastructure upgrades and port physical security are complex concerns and creating early partnerships facilitates seamless preparedness and response. Coordinating research and development activities improves capabilities and uses the limited number of resources available effectively. Every local government and seaport operates differently. However, all do have something in common; they meet regularly with law enforcement officials, work together to modify and update security plans and participate in a variety of exercises. First responders, such as the police and fire departments, receive training and equipment funds from local leaders, sometimes through grants. Local exercises involve public stakeholders to include elected leadership and

local FEMA officials and private stakeholders such as port tenants, law enforcement and first responders. Many local governments have some type of operations center where leaders across all agencies coordinate and communicate with one another (DHS 2008).

Local leaders are required to develop partnerships and conduct exercises. At the local level, an Emergency Manager coordinates preparation, response and emergency services. Local leadership establishes relationships with volunteer organizations, which play a critical role during incidents. Executing training and exercises with all key agencies, law enforcement and emergency services tests plans and response protocols and facilitates necessary updates to plans and modifications if required.

Providing Oversight

Responsibility resides with all levels of government as well as the private sector for conducting assessments, making upgrades and improvements and analysis. However, identification of the department, agency, or level of government responsible for providing oversight serving as the honest broker between all responsible parties requires a review of the numerous regulations and policies. Numerous federal documents, policies, and directives identified the DHS as the department that is responsible for providing oversight concerning maritime security. The United States Coast Guard (USCG) is the action agent for DHS providing oversight and is the authority in reference to risk reduction measures and security measures (TWH 2005). The USCG synthesizes all port plans and combines area specific assessments, which lists specific risks. A DHS hierarchical structure exists. As illustrated below in figure 2, the Secretary for DHS coordinates and supports efforts of a team, which is located down to the field level.

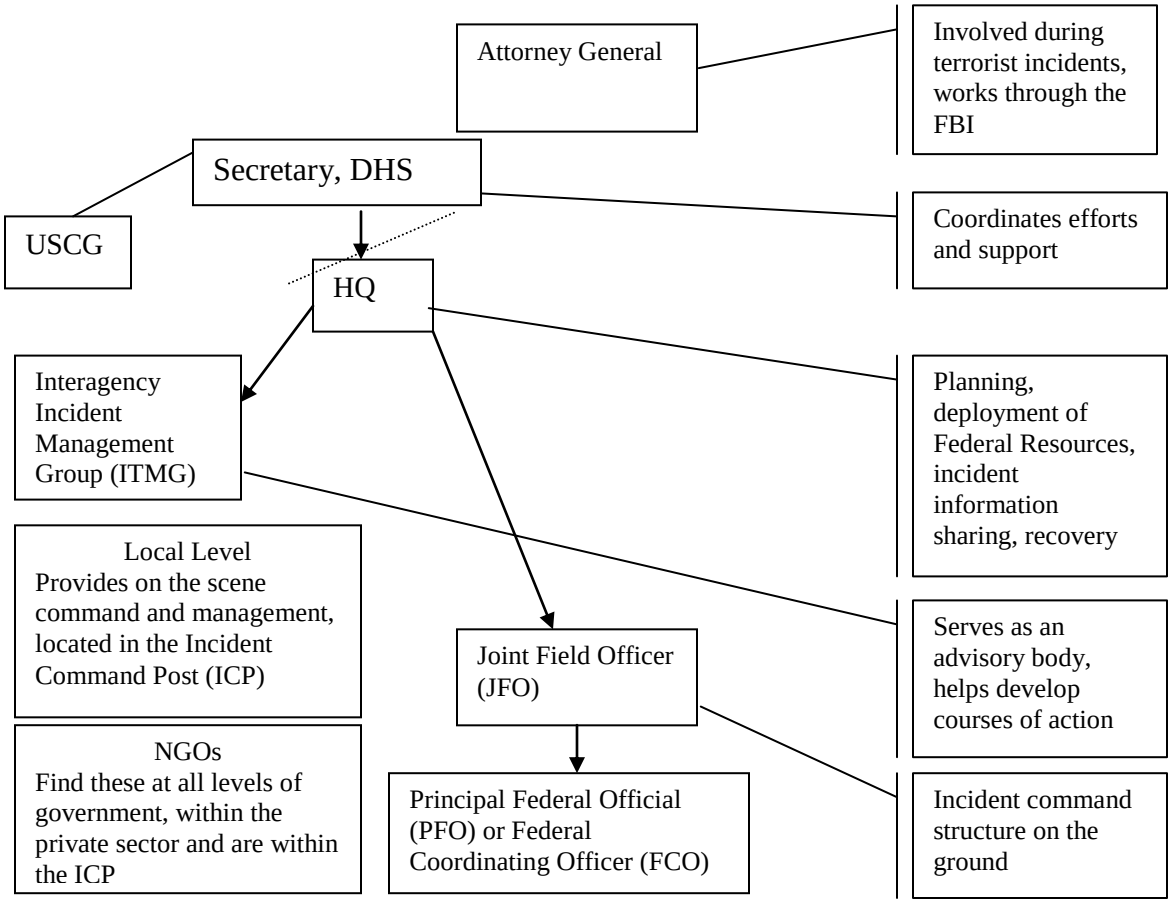

Figure 2. Author's graphic based on information from National Response Framework.

Using the diagram above, it is evident that DHS has representation and coordination between all levels of government. DHS is able to flex if needed and its structure facilitates oversight down to the local level of government. DHS does have programs underway to assist with the implementation of layered security for which the private sector must be involved. Every port is different and therefore has different vulnerabilities. Just a few differences include city infrastructure, population, and state

regulations. DHS has a daunting job of validating oversight of over 300 ports when each creates and implements security and protection measures differently. DHS and DOD must work closely together facilitating oversight while at the same time not stifling economic growth. In a GAO Report entitled *Combating Terrorism: Actions to Improve Force Protection*, it was identified that Port Readiness Committees at each strategic port provided a common coordinating structure for DOD, USCG, and other federal, state and local agencies at the port level for the movement of military equipment (GAO 2002). Although this study focused on DOD and the movement of its cargo, there are similarities between how DOD and private industry handles cargo in relation to port security. All the ports visited for this study applied elements of risk management differently. Individual organizations at the seaports conducted separate vulnerability assessments. This illustrates the need for oversight by DHS at all levels of maritime security.

Although there are field offices which work at the local level, in reality it appears that self-regulation and reporting occurs. According to a CNN article entitled *US Ports Vulnerable to Terrorists*, United States Customs and Borders Protection Agency are not required to use external audit procedures (CNN.com 2008). The article cited a GAO report, which urged requiring consideration of third party and other outside audits and to take steps to make certain companies comply with additional security requirements as needed (CNN 2008).

Existing Doctrine

In order for any branch of government to provide oversight, doctrine must exist that provides guidelines and processes for which to operate within. Numerous federal

documents lay the foundation that focus on plans, execution, incident response and management. Strategic maritime security documents were created and improved over the years. Other detailed plans are derived from the NRF. Many of the plans to include the AMS, the TSSP and the MIRP address and provide guidelines for incident response and management, recovery operations and restoring services such as transportation. Figure 3 illustrates the various plans.

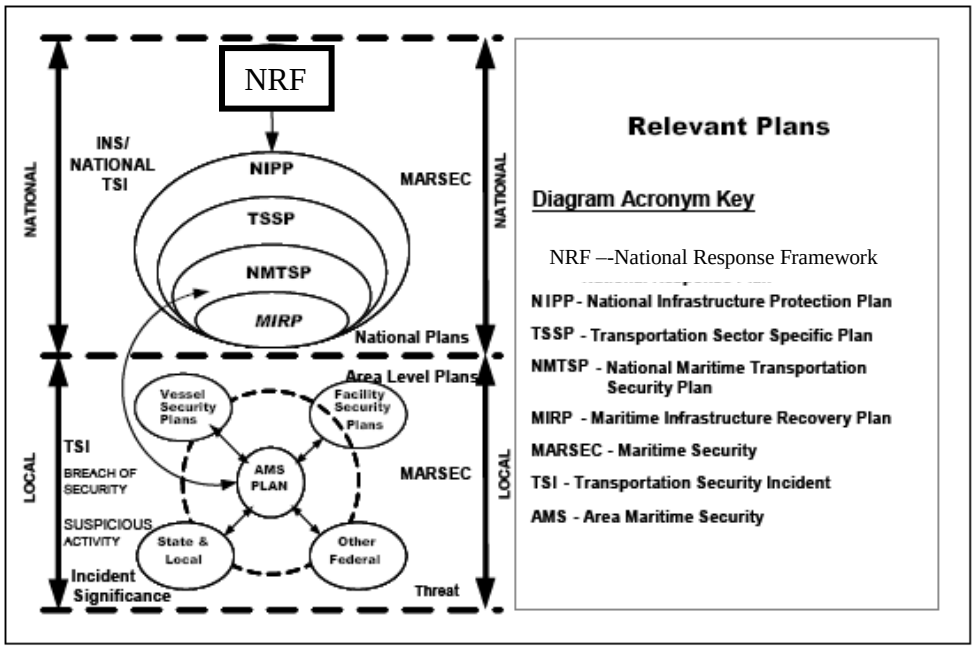

Figure 3. National Strategic Documents Diagram
Source: The White House, *Maritime Infrastructure Recovery Plan for the National Strategy for Maritime Security* (Washington, DC: Government Printing Office, 2005), 24.

Although those are key documents, the NSMS provides guidance on the prevention of attacks, creating domain awareness, interdiction responsibilities, and response to incidents. The NIPP is another document, which addresses prevention and

protection of the maritime domain. Finally, the NMSP presents guidance on maritime security. This document provides information on relationships amongst all levels of government and their responsibilities. By assigning responsibility, key players understand their role and responsibility in providing oversight and creating and implementing doctrine.

Existing national strategic documents contain guidance on prevention, preparedness and responsibilities for each agency. Many documents address incident response actions and coordination between agencies. The private sector owns the majority of shipping containers, which change hands several times before reaching the United States. United States ports and its agents are dependent on information provided by shippers. There are a few regulatory suggestions that would assist in detection prior to ships and their cargo reaching United States seaports. These include Customs-Trade Partnership Against Terrorism (C-TPAT), Container Security Initiative (CSI), and Maritime Transportation Security Act (MTSA). CSI recommends that onboard inspections occur at the port of origin and before getting underway for the United States. MTSA standardizes port security thus making it easier for DHS to provide oversight, regulation, and inspection of over the 300 ports that are on United States soil. Everyone involved in the supply chain are searching for solutions to facilitate protection and inspection without hampering the supply chain (Zeichner Risk Assessment 2006).

Numerous relevant plans exist in order to provide guidance and establish oversight for maritime security. Additionally, there is key legislation to assist in achieving unity of effort. The first is the MTSA of 2002. Objectives of the act are

protection, requiring the federal government to address vulnerabilities and specifying international ship requirements. An additional document is the SAFE Port Act of 2006. The focal points are port security and key programs such as cargo security, screening and credentialing. The SAFE Act established DHS as the responsible federal agency for coordinating intelligence sharing amongst all key agencies as well as developing response plans, creating measurable goals and mechanisms. SAFE Port Act states a port security strategy must address the resilience of the international supply chain and include twelve statutory requirements[1] (Zeichner Risk Analytics 2006). Identification of measurable goals is one of the most important requirements identified.

Both the MTSA and SAFE Port Act focus on unity of effort among all public actors and protection of maritime security. Another key piece of legislation is the C-TPAT. It focuses on security of the supply chain with the Customs and Border Protection Agency as the lead. C-TPAT stresses the importance of creating, coordinating and communicating among all public and private actors. One more law is the Enhanced Border Security and Visa Entry Reform Act of 2002 which permits funding for training of personnel, information sharing, and electronic visas. Finally, this act directs that federal law enforcement and intelligence agencies share intelligence information and use compatible communications systems.

[1]Ten elements were suggested from the importers and two were from carriers, therefore this was entitled 10+2. The two carrier items were, required vessel stow plan and container status messages. The ten items that were suggested by importers included: manufacturer name and address, seller name and address, buyer name and address, ship to name and address, container stuffing location, consolidator, import record number, consignee number, commodity and administrative information such as name, address and port of origin.

Understanding doctrine, legislation and national strategic plans is critical at the local level. It facilitates comprehensive and compliant documents at local levels of government. According to the National Response Framework, criteria for successful plans include acceptability, adequacy, completeness, consistency, feasibility, flexibility, and interoperability (DHS 2008). These criteria were used when comparing the Port of Long Beach and the Port of Miami-Dade.

This section answered the secondary question of how does the United States provide security. The United States has a solid foundation established for maritime security. DHS is identified as the agency that provides oversight and the USCG is the action agent for DHS. DHS coordinates with numerous agencies to include federal, state, and location governments and private stakeholders. Due to the variety and vast differences between ports, DHS is challenged when validating these ports. A large number of federal documents and legislation exists providing guidance and directives on what a port's responsibility consists of, funding and other processes. Strategic documents spell out required relationships, intelligence sharing and security of the supply chain.

Protection Measures

In the previous section, information presented addressed the first secondary question: how do we provide security? The section delved into three subsections, which provided insight into the relationship between the local government and emergency services. Also presented was which agency maintains responsibility for security oversight and the doctrine that exists. This section is an exploration of the next secondary question: what current protection measures exist? Two questions provide

details on this secondary question. What are the United States protection measures, are they tied to the national threat advisory levels and what is the strategic equipment currently used?

Protection Measures and Threat Levels

Throughout the literature review, an examination of dozens of documents, texts, topical websites, newspapers, and national strategic documents occurred. These documents suggested that the federal government has the primary responsibility for ensuring public safety and providing alert information and protection measures. The federal government is responsible for the timely and accurate dissemination of information on which state, local, and tribal governments can act. However, nowhere in the numerous documents was it ever suggested that seaport protection measures exist nor if they are linked to the national security levels. NSMS states domain awareness and layered security includes prevention, protection, and integration actions. This document even provides specific initiatives to maximize domain awareness; however, neither this document nor other strategic documents specifically address maritime protection levels.

Although there are no specified or separate maritime domain security levels, the DHS utilizes the Homeland Security Advisory System. It is a five-level, color-coded threat condition indicator used to communicate the threat condition. The Homeland Security Presidential Directive 3 (HSPD-3), *Homeland Security Advisory System*, created the advisory system to inform all levels of government, its agencies and the public of an overall threat level (DHS 2002). However, DHS can designate a specific geographic region or industry if needed, therefore a separate maritime security threat level system is

not needed and if one existed would pose confusion to those not familiar with the two systems. Utilizing one system allows all agencies to communicate the same message.

Equipment Currently in Use

Terrorists have taken advantage of criminal smuggling networks to circumvent border security measures (TWH 2005). It becomes critical that we as a nation reach across all sectors of government and the private sector to continue research and develop viable strategic protection and prevention options. Several exist although fielded on a small scale. The NRF published in 2008 stated local, tribal, state, and federal jurisdictions need to establish a common understanding of the capabilities of distinct types of response equipment (DHS 2008). The large number of stakeholders prevents coordinated efforts towards procuring effective and common equipment. Monetary resources are a constraint and therefore by reaching across all stakeholders, pooling of resources makes possible the procurement of relevant equipment. Continued research and development exists and new initiatives are underway.

There are numerous initiatives with the first being Operation Safe Commerce. This initiative addresses container screening and better technology. It suggests improving detection at the port of entry and improves the ability of customs agents to conduct searches for illegal cargo. Another is the Container Security Initiative that increases the detection at ports of origin. This initiative's focus is on increasing detection prior to departing the port of debarkation. Finally, under the Cargo Container Security Strategy, the goal is to embed security into commercial practices. United States Customs and Borders Protection Agency along with DHS initially instituted the 24-Hour Rule in

which cargo inspection at port of debarkation occurs at foreign ports at least 24 hours prior to debarking for the United States. The 24-hour prior notification increased to a 96-hour notification in 2003. All high-risk cargo is inspected, however defining what is high-risk cargo is a challenge due to limited resources. Inspection of all high-risk cargo occurs, however the challenge becomes in identifying all high-risk cargo. Due to limited resources, a system-to-system approach is suggested. This links all tools together so that the right asset gets to the right person at the right time.

Monetary and technological initiatives provide the umbrella for continued R&D, testing, and fielding of equipment. While initiatives facilitate the R&D process, equipment outputs exists. The first fielded output is x-ray and gamma-ray screening and non-intrusive inspection technology. Discussion within various topical websites and newspapers presents the benefits and drawbacks of this equipment. It is not relevant to this research as its focus is on nuclear weapons and radiological material. However, relevant technology exists such as Chemical and Biological smart tickets and the Domestic Preparedness Program facilitates providing these supplies to first responders. The tickets detect and/or identify specific agents. Currently, utilization of tickets occurs at the port of embarkation. However, in order to prevent strategic incidents and prevent CW/BW agents reaching United States seaports, it should occur at port of debarkation. Similarly, the National Plan to Achieve Maritime Domain Awareness suggests that development of standoff detection capabilities is necessary to protect the United States shoreline and its seaports. Sensors may be deployed a number of ways to include airborne methods, on buoys or on offshore platforms. One type of sensor is the

BioAttack Early Warning System (BAWS) (Abt Assoc. 2003). It is a defensive measure which attempts to obtain early warning and is capable of detecting BW agents within hours. In the executive summary of the economic Impacts of Bio Terrorist Attacks, the recommendation is to spend $10 billion towards such defense equipment as BAWS. An article in the Washington Times entitled *To Make Sea Traffic Transparent* suggested creating shore based receivers, which interlinks all levels of national and international governments facilitating catching the enemy effectively (*Washington Times* 2008).

Along with new initiatives and R&D, a range of equipment fielding exists at the ports. Frequent discussion occurs on cargo container integrity, security and awareness on security compromise. Because of this focus, numerous types of equipment are available. The first piece of equipment in this area is Anti-tamper Seal, which allows the user or inspector to detect the opening of a shipping container. A wide range of anti-tamper seals exists and include those that record when and by whom a container is opened to having "fingerprints" which are updated whenever a container is opened. Many suggest that having anti-tamper seals increases agent detection prior to arriving at within the range of the United States shoreline. In turn, this could prevent contamination and a large-scale incident. Another piece of strategic equipment is the smart box, which provides information on whether or not containers have been tampered with. Connected to an electronic security device, this is an internationally approved piece of equipment, whose purpose is deterrence and detection of a tampered container. Finally, the Ship Security Alert System (SSAS) serves as a response mechanism which sends an alert to shore indicating any compromise of a ship's security.

Besides physical equipment and development, the creation of computerized systems presents new technological improvements geared towards maritime security. The first includes computerized search tools such as global positioning systems (GPS) and global system for mobiles (GSM) which sends a signal to a control center if a container is opened (RAND 2003). Installed inside the container, these systems can provide a continuous update on a container's location or a periodic update. The two drawbacks are that each system is extremely costly and global coverage is not available. Other technology is the Radio Frequency Identification, which detects inconsistencies in container contents. It also tracks cargo while still within the shipping system. Finally, the Automatic Identification System (AIS) is an awareness tool. This is a vessel tracking mechanism that tracks and monitors vessels. It provides continuous tracking of the whereabouts of a vessel. A final piece of equipment is The Transportation Workers Identification Card (TWIC). It focuses on awareness and prevention. It is a uniform access badge which avoids creating multiple and redundant cards. TWIC is the standard across the United States and implementation is in progress.

This secondary question answered what current protection levels exist. HSPD-3 established the Homeland Security Advisory System and is used to inform public and private sectors to the current risk of enemy attacks. Numerous initiatives, equipment and technology exist or are in the R&D process. Equipment development focuses on screening cargo and containers, increasing detection at ports of origin, embedding security, preventing strategic incidents and establishing computerized tracking systems

for containers and vessels. Monetary resources are the biggest challenge surrounding equipment development and fielding.

The Role of the Federal Government in Protection

The previous two sections provided analysis on how do we provide security and what current protection measures exist? This section is an examination of the final secondary question: what is the role and responsibility of the Federal Government/Homeland Security in protection? Supporting questions that tackle this secondary question are discussed. These address who provides threat analysis/information to those responsible for oversight, who provides funding, how is the money distributed and finally what is the relationship between the local and federal governments?

Providing Threat Analysis

Coordination is required between all levels of government, first responders, and the private sector in order to facilitate seamless and effective cooperation, preparedness, and response. To combat CW/BW weapons, strategic plans must first focus on prevention. Monitoring efforts of suspicious activities, threat analysis, synthesis of information and distribution of information facilitates coordination and communication amongst all actors. The SAFE Port Act designates DHS as the primary office responsible for coordination and communication between all players. DHS is responsible for intelligence information sharing and setting up lines of communication between all levels of government and the private sector.

While DHS is responsible for intelligence dissemination, it shares the responsibility for situational awareness capabilities with DOD and DoJ. These capabilities integrate not only intelligence, but also reconnaissance, navigation systems and other operational inputs. Required access to information should occur at all levels of government, a variety of governmental agencies and the private sector. Access to and sharing of additional pertinent information within their respective area of operations occurs as well.

Although DHS is overall responsible for intelligence information oversight, the FBI, CIA, NSA, and local police are responsible for collection of information on and interdiction of enemy activities. Prior to 9/11, FBI's primary focus was on law enforcement, not intelligence; therefore, it does not have experience in producing threat assessments. Additionally, local levels of government do not have access to the information the FBI gathers. Communication tools are available and used, however coordination between agencies is lacking. State and local governments as well as the private sector have stated that the information they receive from the federal government is often unclear, conflicting or duplicated (TWH 2003). Information filtered down to users is often late or the agency that needs the information cannot access it due to security measures.

The primary method for information sharing, situational awareness, and collaborative planning will be the national maritime common operating picture (COP) (TWC 2005). The National Maritime COP is the primary means for disseminating maritime domain awareness (MDA). Utilizing the COP enables analysis and integration

of the large quantity of incoming data and provides actionable and credible threat information. The Homeland Security Act of 2002 eliminated many of the legal obstacles that prevented access by the private sector and many public sector agencies. Additionally, in accordance with Executive Order 13356 and the Intelligence Reform Act of 2004 it establishes legal authorities, interagency agreements and policies to allow the processing and fusion of foreign intelligence, domestic law enforcement information and commercial data sharing (TWH 2005).

There are a variety of agencies involved in providing threat analysis although DHS is responsible for oversight, a variety of agencies are responsible for collection of potential threat and suspicious activities and interdiction of these actions. The USCG plays a vital strategic role in MDA. The USCG also collects, analyzes and disseminates information. This information feeds into the COP; however, the process is still at the beginning stages and needs work. The importance is linkage between actionable threats and the COP. What occurs at each port can have a strategic impact. Cooperation is required at all levels of government, all agencies within government, with the private sector and with first responders in order to integrate all sources of intelligence information.

Ensuring all agencies use the COP for disseminating information simplifies coordination amongst the numerous and varied agencies. One tool that feeds into and receives a lot of attention is container security. The important piece of container security related to this thesis is the involvement by the National Targeting Center (NTC). The Customs and Border Protection Agency uses the NTC as the central coordination point

for anti-terrorism efforts. The Customs and Border Protection Agency coordinates with the USCG, FBI, Federal Air Marshals, Transportation Security and the intelligence community for advance information on suspicious cargo.

Although DHS has responsibility for oversight and numerous agencies have responsibility for collection and dissemination, it is every agencies' continued responsibility for conducting vulnerability assessments, and submitting information on any suspicious activities for analysis. Many private interests created sector coordinators and established Information Sharing and Analysis Centers (ISAC). The Physical Protection of Critical Infrastructure and Key Assets plan inferred that ISACs serve as a good model for public-private sector information sharing. Although ISACs have a proven record of accomplishment for information sharing, they lack advanced analytical capabilities that DHS and other federal agencies have.

Funding

Success of the maritime security program hinges on proper funding. Who provides the funding and how it is distributed are the key questions. The federal government has increased its spending. However declines in revenues at the state and local levels of government increase the need for federal assistance. Collaboration is required at all levels to ensure requirements are resourced and to reduce redundancies. An article by the Heritage Foundation suggests that because "the United States infrastructure is largely in private sector hands, public-private partnerships should be constructed to maximize cooperation and minimize disruption… and any attempts to create these partnerships must first resolve who pays for threat analysis and response"

(Heritage Foundation 2005). Applications and requests for funding are problematic. There are duplications in a convoluted system and the review process can be long when a cross agency review is required.

With local and state revenues declining and the threat increasing, a resource need exists. Several programs make funds available. The first is the Stafford Act, which focuses on providing funding for incident response, not for prevention or protection efforts. However, the C-TPAT provides incentives to the private sector if they participate in C-TPAT. A Brookings Institute article suggests that instead of spending billions of dollars on a long-range missile defense program; at least part of these funds should be diverted to maritime protection where funding is woefully inadequate (Brookings Institute 2001). It further goes on to suggest that monetary resources should be spent on training and protection equipment (Brookings Institute 2008). There is a need for new financing options. One study conducted recognizes that [local government leaders'] mission is not only to identify one source of funding but also describe the need for funding… among these options are expanded eligibility for existing TEA-21 programs (National Chamber Foundation 2003). There are no grants or monetary resource specific items found in the SAFE Port Act or the NIMS; however, the Transportation Security Administration (TSA) funded the TWIC prototype at $50 million, which has now become the standardized card at every seaport. The Enhanced Border Security and Visa Entry Reform Act of 2002 addresses funding for training, increased pay for employees and made $150 million available to improve technological capabilities. It is also noteworthy to mention that this act approves of states charging a fee or a higher rate for those non-

machine readable passports as a way to generate revenue. Finally, Port Security Grants are available for projects involving facility improvement and operational security. From 2001-2005, the federal government distributed over $556 million in grant money. Considering the amount spent on other areas of homeland security, this amount seems inadequate. The Port Security Council identified $400 million needed for FY 2006 and $5.4 billion needed funding through 2012 (Port Security Council 2006).

Numerous programs and funds are available for distribution to those ports that apply for them. However, the hard-to-navigate system makes it difficult for local leaders to obtain funding. There are grants available and state and local leaders should maximize these resources. In the case analysis, applying for more grants is better as it facilitates completing projects in a variety of maritime security areas, infrastructure projects and communication tools.

Relationship Between Federal and Local Governments

A harmonious relationship must exist between governments at all levels in order to ensure successful maritime security. The *National Response Framework* provides structures for implementing strategic policies and coordination. The SAFE Port Act requires DHS to describe the roles, responsibilities and authorities of public and private stakeholders, provide measurable goals, objectives and mechanisms (Heritage Foundation 2005). A Heritage article entitled *Making the Sea Safer* emphasizes the importance and criticality of creating public-private partnerships to minimize trade disruption and increase protection (Heritage Foundation 2005). DHS ensures coordination occurs with the USCG, Customs and Border Protection and other federal agencies who in turn will

coordinate and provide information to the private sector. The chart below illustrates coordination and communication between the federal governmental agencies, local leaders and the private sector. Partnerships between local, state and federal agencies and leadership exist as illustrated. Additionally, partnership with NGOs and private sector stakeholders are tied at all levels. There are numerous coordination groups and public-private associations as the diagram depicts in figure 4.

The Joint Field Office (JFO) is the primary federal incident management structure. It is organized, staffed, and managed in a manner consistent with NIMS principles and is led by the Unified Coordination Group (DHS 2008). The JFO provides the structure to integrate and coordinate response and recovery activities. The Unified Coordination Group consists of the Principal Federal Official, the State Coordinating Officer, Federal Coordinating Officer and other senior officials from additional federal agencies and representatives from state and local governments (DHS 2008). Partnerships exist with state and local officials and EOCs at every level as well as with non-governmental organizations, which facilitates planning, response and recovery activities. The JFO establishes a Joint Operating Center (JOC) and includes the Domestic Readiness Group and the Counter-terrorism Group.

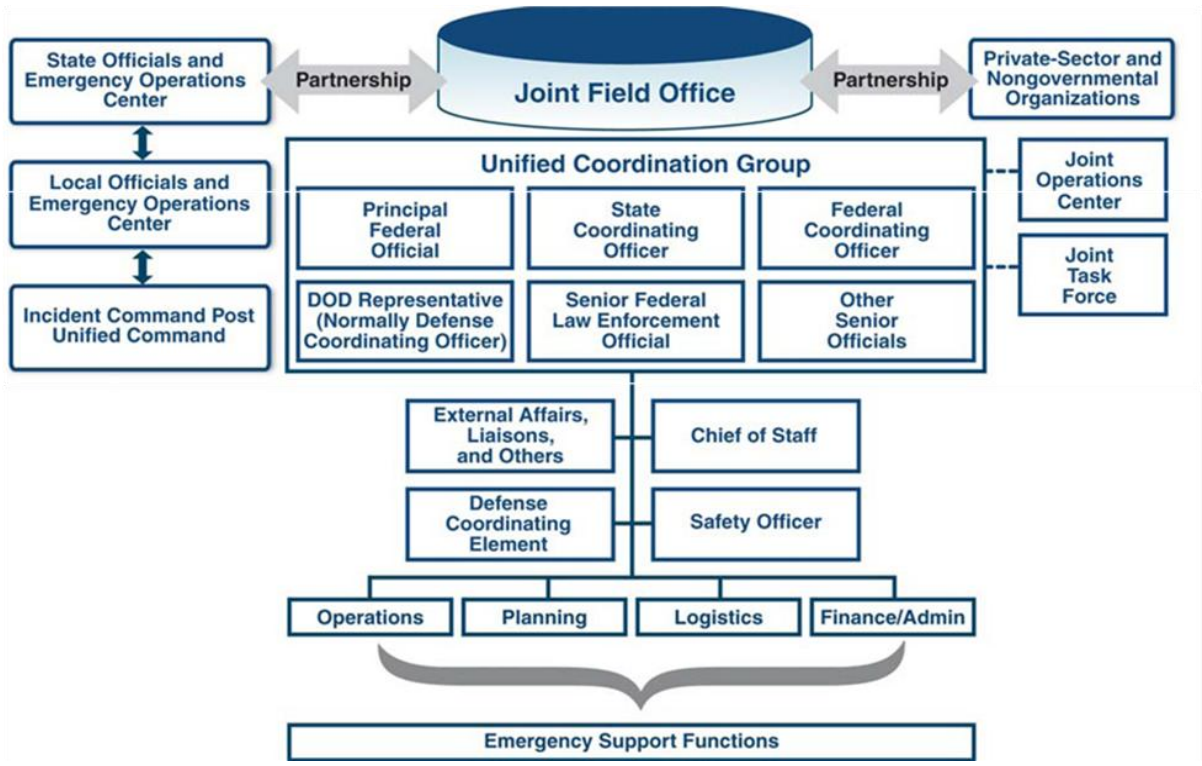

Figure 4. Coordination Chart
Source: DHS, *National Response Framework* (Washington, DC: Government Printing Office, 2008), 63.

The federal government continues to build its relationship with state and local responders through partnerships. At the federal level, two groups are established that convene on a regular basis to develop and coordinate preparedness and response policies. The first is the Domestic Readiness Group, which evaluates and makes recommendations on policy issues. The second group is the Counter-terrorism Group, which develops policies, response to terrorism, and coordinates law enforcement investigations associated with terrorism. The National Operations Center (NOC) serves as the primary center for coordinating operations across the federal government and its agencies. The NOC provides DHS and other principles with information necessary to make critical decisions

(DHS 2008). The Secretary for the DHS provides information and ensures dissemination of information throughout all channels. The Secretary for Homeland Security also coordinates all federal resources and works with State Governors and the State Homeland Security Advisor for any federal assistance needed. Finally, the JFO is the primary response office operated when an incident occurs. It serves as the central coordination location between all levels of government and private sector stakeholders and the focus is response and recovery. However, the JOC operates daily and coordinates activities and assets in preparation for, response to, and resolution of an incident.

At the federal level, the Secretary for DHS serves as a conduit between federal and state levels of government. The State Governor plays a key role in this relationship, not only coordinating for resources, but its priority is to supplement local government efforts. S/he coordinates state resources, commands the state military force and coordinates assistance from other states as needed. Although congressional leaders do not in fact run the state, they serve as a resource that both local and state government leaders employ. Congressional leaders provide guidance in understanding federal resources that are available. Every state maintains an Emergency Operations Center (EOC). During an incident, the local level maintains responsibility, but it is at the state EOC where coordination occurs between a multitude of agencies.

Federal and State leaders play supporting roles and assistance to local leaders. Local leaders not only have the responsibility of coordinating with state agencies and private stakeholders, but also communicating with the public on preparation and response. Many private agency stakeholders operate and maintain port infrastructure,

therefore it is imperative that relationships are established and coordinate and create plans prior to an incident. The local appointed/elected official can directly coordinate with members of congress, non-governmental organizations, the private sector as well as other local leaders. Besides local response agencies and law enforcement officials, the local appointed/elected official has a team of experts such as an Emergency Manager that assist in coordinating and communicating preparedness and response policies. The Emergency Manager oversees day-to-day emergency programs and preparation.

In this section, the protection role of the federal government was defined. The COP is a tool employed by all stakeholders. It provides visibility on all potential threats and DHS is responsible for its oversight with a variety of actors serving as intelligence collection agents. The drawback is obtaining access, however the Homeland Security Act of 2002 eliminated many of the legal obstacles. Much legislation exists which facilitates grant programs for ports. However there is a shortage of funding available. DHS provides guidance on the roles and responsibilities of all stakeholders involved in maritime domain security. Working groups exist at all levels facilitating coordination with private stakeholders at all levels of government.

Case Study of Two Ports

The two ports selected for the case analysis are Port of Long Beach located in California and Port of Miami-Dade located in Florida. Situated on different coasts, these ports have different population sizes and location but similar economic importance and are large enough to conduct research and analysis. This section is an analysis of each port using the secondary and tertiary research questions. Finally, a case study

comparison chart summarizes the information of both ports and compares them side-by-side.

Port of Long Beach

The Port of Long Beach is the second busiest port in the United States and the fifteenth busiest container cargo port in the world. The top imports are petroleum and plastics while the top exports are petroleum products and chemicals. The shipping terminals provide approximately one-third of the waterborne trade moving through the west coast and the port generates $15 billion in annual trade related wages (Port of Long Beach 2008). The port is self-supporting financially. It does not receive tax revenues or money from the city's general fund (Port of Long Beach 2008). The port is a landlord port, which makes money by leasing facilities and is the principal revenue source. California tidelands laws require ports to earn and spend their revenues only on activities related to commerce, navigation, marine recreation and fisheries (Port of Long Beach 2008).

Doctrine and Interagency Relationships

The Port of Long Beach is a public agency. Although operated by the City of Long Beach, specifically the Harbor Department, it is governed by a board of commissioners. The governor appoints the five-member commissioners' panel. The port cannot outsource security to private companies due to the responsibility and jurisdiction of many government agencies. Prior to 9/11, the focus was on preventing cargo theft but now antiterrorist security is at the forefront. Focus on security is more intense, more focused and involves more organizations. The Port of Long Beach has a wide variety of

security partners with the primary objectives of securing containers, terminals and the coastline. The various partnerships established include the USCG, Customs and Borders Protection Agency, State Homeland Security office, Federal DHS, Long Beach Police Department and the Port Harbor Patrol, which includes a port dive team.

The Port of Long Beach created a ten-year strategic plan that outlines among other items, port safety and security, industry and government relations and infrastructure. Between the years of 2002-2006, the port received $35 million in federal grants, which the port used to enhance communications systems and security technology (Port of Long Beach 2006). The port also used the funds to increase outreach efforts with the purpose of public education. Annual Business Plans produced by individual port divisions will translate strategic plan strategies into actionable programs and objectives that can be measured each year (City of Long Beach 2006). Both bi-annual reviews and yearly division reviews enable the port to assess measurable goals and evaluate performance. The strategic plan outlines several critical areas and the strategies to help achieve overall maritime security. The plan details specifics in the areas of safety and security, community, industry and government relations, infrastructure and transportation, financial strength and organizational effectiveness.

Application of Doctrine and Plans

All terminals must abide by the Federal Maritime Transportation Act of 2002 (FMTA). The FMTA indicates that those private companies who lease facilities and contract with union long-shore workers to operate shipping terminals must adhere to federal guidelines. The port underwent an audit in 2004 and again in August 2007 by the

Customs and Border Protection (CBP) Agency. Audits are conducted due to the port's involvement with C-TPAT, which the port elected to join in 2003. These audits provide their security profile. The security profile listed the security procedures the port currently had in place. In February 2004, CBP validated the Port of Long Beach's strategic plan as required by C-TPAT, which requires re-validation every four years. As indicated throughout all the documents and the port's website, a few exercises were conducted but there was no consistency.

Funding

The port must spend monetary resources in accordance with the guidelines established by the California Tidelands laws and the Long Beach City Charter. Therefore, the port must manage funds strategically focused on long-term goals. As of February 2008, the total grants received from the state to the port totaled $9.2 million and from the federal government over $50 million (Port of Long Beach 2008). The port received $8.4 million in security grants from the State Homeland Security Office in early 2008 (Port of Long Beach 2008). The port distributed grant money received to those infrastructure improvements and equipment needs across all agencies including first responders. The port will use the grant for the following projects: security stakeholders system, disaster recovery center, public address system, radio frequency identification system and camera for harbor patrol, police and fireboats (Port of Long Beach 2008). A recent $20 million command and control center opened serving as a type of emergency operations center. Although funded by the Port of Long Beach, DHS contributed over $8 million towards the center. This is the first time that all partnership agencies will work

under one roof. Additionally, security improved due to low cost improvement measures such as fixing fences and repairing locks. However, improvements need to be made in the areas of container security and coastline protection (The CalTrade Report 2004). During the first year federal funding was available, the port received $4.3 million that went towards installing cameras and surveillance equipment, crash barriers and fences. The port bought 60 Hazmat suits for protection against CW/BW agents. However, the City of Long Beach did not schedule training until three years later.

In addition to infrastructure improvements, R&D projects continue. The port bought gamma and x-ray scanners and radiation portal monitors. Unfortunately these scanners and monitors do not scan for CW/BW agents. The port is working with international partners to develop container locking devices and GPS tracking devices. Ships entering United States coastal waters are required to report 96 hours in advance in accordance with the Container Security Initiative. The port started using a new intrusion barrier entitled small craft intrusion. These barriers, originally designed for erosion control, protect against intrusions and entry by threatening vessels. The Maritime Transportation Security Act and the SAFE Port Act require ports to use the TWIC. The Port of Long Beach was one of the thirty-five ports which participated in the test pilot program. This facilitates more background checks on all workers to including truck drivers. One of the technologies the port is considering is the electronic smart lock located on containers and sends an electronic signal if a container is opened enroute to the United States; however funding is still an issue. Senator Alan Loventhal said due to an increase in costs associated with procuring these types of technologies, he wants one-

third of the money proposed to be raised by container fees which would go to the ports for security (Grunion Gazette 2006). Estimated revenue generated totals over $166 million each year, however the governor needed to sign the bill (Grunion Gazette 2006).

While the port has received a substantial amount of federal grant money as well as state grants, Senator Feinstein insists an overhaul of some legislation is required. The senator has teamed up with Long Beach Mayor, Long Beach Police Department Chief and the Los Angeles Mayor to call for the passing of two key pieces of federal legislation. The purpose is to call for harsher criminal laws and request that federal funding and awarding of grants based on threat versus geographical or political areas. Finally, the Senator proposes a Homeland Security bill, which requires DHS to allocate grants based on risk and funding to meet essential capabilities by reducing vulnerability to attacks and diminishing them (Senator Feinstein 2008). Current practice allocates equal distribution of thirty-eight percent of the funds to each state before any analysis and the proposed Feinstein bill calls for the elimination of equal distribution.

Port of Miami-Dade

Port of Miami-Dade is the third largest international passenger traffic port in the United States and is one of the largest open sea borders with over 20 miles of coastline which makes it easier for an enemy to conduct terrorist activities. In 2007, approximately 8 million tons of cargo passed through the port (Miami-Dade County 2008). By 2020, it is expected that most United States container port gateways will double or triple in volume (Port of Miami-Dade 2008). Due to this, the port's focus is on improving infrastructure and connecting to the city of Miami and interstate access.

Doctrine and Interagency Relationships

The Maritime Transportation Security Act states that collaborative planning between county and ports should occur. The port established critical relationships with first responders' statewide and multi-agency partnerships. The port established the Domestic Security Oversight Council, which serves as the executive policy advisory group. Participants include the Florida Department of Law Enforcement, Florida Division of Emergency Management, heads of state agencies, representatives from federal and private sectors, regional domestic task forces and professional partners. The group is charged with developing and annually updating the domestic security strategy. The four goals of the security strategy are to prepare for terrorism response missions, prevent, preempt and deter acts of terrorism, protect Florida citizens, visitors, and critical infrastructures, and respond in an immediately effective and coordinated manner (Florida's Domestic Security Annual Report 2007). Several initiatives include the federally mandated NIMS training and hardening infrastructures, which the Port of Miami-Dade has and continues to implement.

Compliant with strategic guidance, local plans are reviewed annually. Florida created a fusion cell that enhances information sharing, intelligence capabilities, preparedness operations and connectivity among all Florida regions. The Port of Miami-Dade experienced what was perceived as a potential incident in 2007 when three men attempted to enter a secure area without proper documentation (CNN.com 2007). Implemented several years ago, the TWIC served as the first indicator of a potential incident. Multi-agency coordination occurred between the FBI, port authorities, Immigration and Customs Enforcement and the USCG and finally cargo scanning

occurred during this incident. This incident illustrates that plans, processes, interagency relationships and response mechanisms exist.

Application of Doctrine and Plans

Initially, the plan was not compliant with NIMS; however, the Comprehensive Emergency Management Plan and Terrorism Annex was comprehensive and compliant (Domestic Security Oversight Council 2007). The state worked diligently to meet regulatory guidance consistent with federal guidance and policies. The port continues to make progress on port security. The federal government launched the Homeland Security Initiative at the Port of Miami-Dade. The port completed numerous domestic preparedness exercises. One exercise allowed TV students from the local community college to participate. The students documented the multi-agency exercise where simulated CW/BW attacks occurred. Included were inter-agency partnerships and response actions by fire and law enforcement agencies. Other exercises include first response exercises where responders had to react to a full-scale WMD exercise involving CW/BW agents. Additional exercises consisted of port tabletop exercises, governor's tabletop exercises, regional task force exercises, coordination exercises with government agencies, and other WMD exercises.

Funding

A strategic plan exists and the port continues to comply with federal guidelines and policies. In the area of funding, the port previously spent $11.5 million each year to protect the port and now it spends $18 million annually which is more than any other state spends on security (Miami-Dade County 2008). Additionally, private partners

spend millions on their own security systems. The goal should be to integrate into one system which saves monetary resources while at the same time facilitates coordination. From 2002-2005, the port received less than twelve percent of all the country funding applied for from both state and federal governments. The significance is that $280 million was identified as needed for homeland security creating a shortfall of $116 million therefore a list of unfunded requirements exists. The port has received federal grants for capital improvements. To date, the port applied for $646 million and received $80 million in grants (Miami-Dade County 2005). The funding was used in a variety of ways to include training and equipping first responders, conducting vulnerability assessments, infrastructure hardening, and security enhancements and upgrades (Domestic Security Oversight Council 2007).

The port states that funding allocation is strategically based to achieve preparedness, response, recovery and mitigation. Funds received were allocated to training first responders, educating the public and obtaining disaster response equipment. The port currently requires an additional $280 million in Homeland Security needs. Priority projects requiring additional funding include securing the port and guarding against water contamination threat.

The Maritime Transportation Security Act and the SAFE Port Act require ports to use the TWIC, which assists with background screening on every individual. Similar to the Port of Long Beach, the Port of Miami-Dade was one of the 35 ports which participated in the test pilot program.

According to the Port of Miami-Dade Freight Access Study, as globalization continues access and capacity needs to expand to meet the demands (Cambridge Systematics 2007). The port and city project $1.2 billion to build a tunnel to the Port of Miami-Dade. Florida DOT will pay $600 million, and other funding comes from the general obligation bond, local transportation fees, city contribution, charging tolls and increasing user fees for cargo and cruise ships. The tunnel project is controversial in that the funds could be used elsewhere and for other physical security upgrades, however the port fees will pay for part of the project, future upgrades and will meet future economic and trade demands. Upgrades of the port security gate included installing software, hardware, and upgrading network communications systems. These upgrades streamlined the port's security gate operations.

Research Matrix

This thesis uses a qualitative analysis approach and a trichotomous rating - completely, partial or not at all to analyze the two ports. Below is a case study comparison chart of the Ports of Long Beach and Miami-Dade. It synthesizes and summarizes the information contained in the two sections above. Overall, each port has made significant strides in preparation, preparedness, planning and increasing operational security and incident response. Table 2 summarizes the comparison between the two ports.

In the area of doctrine and interagency relationships, both ports have local plans in place and attempt to follow strategic guidance. Because the Port of Long Beach volunteered to participate in C-TPAT, it undergoes audits every four years and bi-annual

reviews. After its formation, the Domestic Security Oversight Council began yearly reviews after discovering the plan's shortcomings. Both ports are successful at collaborating with a myriad of agencies including first responders, public agencies at all levels of government, private sectors and colleges as well as improving communications systems. The port of Long Beach recently opened a new command and control center. The Port of Miami-Dade has multiple communications systems in place, which detracts from using one centralized system.

Table 2. Research Matrix Comparing the ports of Long Beach and Miami-Dade

Evaluation Criteria	Port of Long Beach	Port of Miami-Dade
Doctrine and Interagency Relationships		
Local plans written	Completely	Completely
Local plans follow strategic guidance	Completely	Partial
Local government establishes partnerships with private sectors	Completely	Completely
Communications systems in place	Completely	Completely
Application of Doctrine and Plans		
Applied federal documents within local plans	Completely	Partial
Applied legislation within local plans	Completely	Partial
Exercises conducted with local public and private sectors	Partial	Completely
Exercises compliant with federal guidance	Completely	Completely
Training conducted	Partial	Completely
Funding		
Applied for federal grants	Completely	Completely
Budget allocation – R&D	Not at all	Not at all
Budget allocation – Infrastructure Improvements	Completely	Completely

Differences between the two ports exist in the area of doctrine and interagency relationships and continue with how the ports applied doctrine and plans. The Port of Long Beach participates in C-TPAT, thus helping ensure that the port is compliant. While the Port of Miami-Dade had challenges in the past, the creation and use of the Domestic Security Oversight Council chaired by the Florida Department of Law Enforcement and co-chaired by the Department of Emergency Management along with yearly reviews smoothes the progress of understanding guidance and complying with legislation. Unlike the Port of Long Beach, which has conducted minimal exercises, the Port of Miami-Dade conducts a wide range of exercises with different focus for each and involving agencies at all levels of government, first responders, local colleges and private agencies. The Port of Miami-Dade's training program focuses on not only allocating funds for all actors involved in port security, but it also includes training programs and workshops for the local community. The Port of Long Beach appears to have met the minimum training required by legislation, however reaching out to other leaders and agencies within the community assists with preparation and response.

Creating local doctrine, which is compliant with federal policies, guidelines and legislation, is critical and are two aspects of preparedness and port protection. Another vital aspect is funding. Both ports have and intend to continue to apply for federal grants. Areas benefiting from the majority of the grants have been infrastructure improvements and physical security. While the Port of Long Beach most recently finished its command and control center, the Port of Miami-Dade is focused on the new expansion tunnel and the fusion center. Both have equally upgraded fences, camera systems, locks, and gates.

Both have not allocated funding for research and development. Notably, the Port of Long Beach obtained technology in the form of intrusion barriers originally development for other purposes. Long Beach is also considering the electronic smart lock located on containers which sends an electronic signal if a container is opened enroute to the United States.

Summary

This chapter focused on research analysis. The bottom line is that yes, all levels of government do have marginally adequate prevention measures in place. Doctrine at all levels, coordination among all stakeholders, basic funding and protection measures exist. There is not enough information to answer the follow up question of on whether measures help prevent CW/BW attacks. Exploration of secondary and tertiary questions delved into detailed doctrine, legislation and planning at all levels of government. Critical to maritime domain security are partnerships at all levels of government, private sector, local law enforcement agencies and first responders. Intelligence analysis and dissemination is not effective if agencies do not have access to the information and communications networks. Protective measures and equipment currently in use or in development were presented. Funding in the form of grants and budget sets up ports for success in preparedness and response. Upon obtaining information on secondary and tertiary questions, a case analysis between the two ports of Long Beach and Miami-Dade was conducted. Utilizing evaluation criteria and a research matrix, comparison between the two seaports illustrated the similarities and differences of each. Both ports have

strengths and weaknesses; however, each continues to make improvements towards securing the maritime security domain.

Chapter 5 includes the thesis summary, conclusions, remaining research and the way ahead.

CHAPTER 5

CONCLUSION

Introduction

The public and private sectors at all levels have important roles to play as the United States protects its interests in the maritime domain (DHS 2005). The previous chapter emphasized this point in analysis of the maritime security domain. It included in-depth information answering the primary, secondary and tertiary research questions. Additionally, the previous chapter included a case analysis conducted on two ports, one on each coast. This chapter presents conclusions and recommendations based on previous chapters. It is organized to include a brief summary of findings, interpretation of those findings, the implications and recommendations for future port security.

Primary Research Question

The primary question and focus for this thesis is do United States seaports have adequate preventive measures in place to provide early warning to the public? The follow up question to this is if there are preventive measures in place, will they assist in preventing chemical and or biological attacks? The bottom line is that yes, all levels of government do have marginally adequate prevention measures in place. Doctrine at all levels, coordination among all stakeholders, basic funding and protection measures are in place. There is not enough information to answer the follow up question whether there are measures in place that help prevent CW/BW attacks.

Brief Summary of Findings

In order to provide a brief summary and ultimately answer the primary research question, this section is divided by secondary questions. Within each section, the answers to tertiary questions lead to answering the secondary questions and therefore the primary research question.

Providing Security

The first secondary question answers how the various stakeholders provide security. The relationship between local governments, emergency services and first responders is effective. With plans, policies, training and exercises, working relationships have become more efficient. Communication at all levels increased especially with the advent of operations centers and common communications systems.

Along with having a working relationship between local governments and emergency services, there is equal importance in providing oversight. The DHS is the federal agency responsible for oversight concerning maritime security. It coordinates with governments at all levels, USCG, the Attorney General and Joint Field Officers to ensure plans, policies, directives, and funding reaches all levels. DHS works closely with DOD to facilitate oversight.

In addition to working relationships and providing oversight, doctrine and security documents lay the foundation for stakeholders to follow. The key issue is who has ownership of the problem of maritime security. Within national strategic documents and presidential directives, DHS is identified as the key federal agency that is responsible for oversight. Once defined, creation of policy, plans and oversight began. Numerous

doctrines, documents and pieces legislation exist providing the groundwork and guidelines on planning, execution and response for maritime security.

Current Protection Measures

The next secondary question answers what current protection measures exist. DHS did not establish a protection measure system or threat level system for maritime security. DHS uses the Homeland Security Advisory system to inform all agencies and the private sector of a threat increase.

Although there is no specific maritime threat level system, there are various pieces of equipment currently in use or are in the R&D cycle. The private sector predominately explores physical security protection equipment initiatives. Each piece of equipment developed focuses on detection, protection or early warning. The large number of stakeholders and monetary constraints has prevented coordinated efforts toward working together on R&D. The list of equipment ranges from physical, to computer programs to the TWIC. If adopted, these new equipment and technologies are an initial start. Continuous research and development is required in order to ensure continued maritime domain security.

Responsibility of the Federal Government

The final secondary question addressed what is the role and responsibility of the federal government in protection. DHS is responsible for providing threat analysis, monitoring intelligence efforts and dissemination of intelligence information. The SAFE Port Act identified DHS as the primary office for this intelligence role. DOD and DoJ share responsibility with DHS for situational awareness. Intelligence collection involves

an abundant number of federal agencies to include the FBI, CIA, and the local police. The USCG also collects, analyzes, and disseminates information. The maritime COP is the primary means for information sharing and situational awareness.

Intelligence analysis and dissemination is critical in order to ensure stakeholders have the most current information. Funding is also critical to the success of maritime security. Funding is a constraint that all levels of government and private sector face daily. There are grants available and states apply for and receive them under provisions of legislation. However, ports need additional funding.

The local and federal governments continue to build a working relationship through partnerships. There are numerous coordination groups to include EOCs and JFOs. Coordination groups meet frequently to develop and coordinate plans, polices and response actions. Leadership coordination at all levels builds to successful partnerships. Working relationships are demonstrated at all levels among governors, local leaders and DHS. There is a common goal of maritime security even if not a commonality of approach to the issue.

Case Analysis

Analyzing two ports using secondary and tertiary questions demonstrated that these selected ports have made progress. A chart was created in the previous chapter using a trichotomous evaluation that summarized each port's progress towards maritime security. Although each port has its strengths and weaknesses, each made an effort to create an effective and viable maritime domain security program.

Interpretation of Findings

Presented above was a brief synopsis on the analysis conducted in the previous chapter. It is not enough to just present the facts and analyze them. It is not enough just to know the facts, it is also important to understand what the analysis means and the implications from it.

What Results Mean

Overall, the prevention measures currently in place are marginally adequate but more needs to be done. Government at all levels do have plans and processes in place, however they need revised and updated. The legislation, current equipment and the role the federal government assist in preventing a chemical/biological attack. The results identified indicate a number of areas for which emphasis needs to remain. The federal government should continue to provide oversight in the areas of establishing policies, security requirements, and assessing compliance. The federal government needs to serve as the honest broker or security efforts may flounder. A plethora of doctrine and strategic plans exist setting guidelines from which to operate and conduct detailed planning and execute exercises with all stakeholders. The GAO is an effective tool to encourage port compliance. Outside audits assist local leaders with making improvements.

Oversight is necessary but so is a focus on protection measures. Because there are no separate protection levels outside of the Homeland Security Advisory System, there is less confusion amongst all stakeholders. Utilizing one system allows all agencies to communicate the same message. DHS has the flexibility to designate a specific industry or geographical reason a higher level if needed. This again facilitates only

raising the threat level where a possible threat exists versus the additional costs of alerting the entire country. Tailoring resources to a specific area ensures that they are not wasted.

Oversight and unified threat levels are needed but not sufficient. Funding at all government levels is needed but currently insufficient. Initiatives such as C-TPAT, CSI and MTSA focus on prevention and deterrence. The government should continue these. However, the private sector should allocate additional resources to improve continued operations in the event that an attack occurs. The TWIC is standard across all ports and a successful initiative. It eliminates redundant cards and the use of multiple cards for an individual. With the elimination of multiple cards, the resources that were spent on the multiple cards can be shifted to the TWIC system enabling detailed background checks.

Threat and information analysis and its dissemination is improved but incomplete. Agencies are still working out ways to communicate with stakeholders. Legislation exists which assists in eliminating bureaucracy in obtaining current intelligence, but federal agencies still have work to do in this area. Creating a current operating picture for the maritime domain is the first step towards all stakeholders using the same information. By having this system, intelligence dissemination flow occurs simultaneous thus eliminating time delays. The system is only good if all required agencies have access and systems support. Legislation facilitates access, however the process for approval is slow and funding of equipment requires additional time.

A glaring weakness is the scanning and screening process. Some of the technology presented involves screening and scanning at the port of origin, which

reduces/mitigates the risk of acts of terrorism on United States soil. However, some of the technology only screens and scans at a United States port of entry. Although a port can segregate a container, protection is not as high as scanning prior to entry. Increasing the 24-hour rule to the 96-hour rule helped. It required ships to provide load lists and other required information 96 hours out which resulted in additional lead-time for threat analysis. However, an enemy could always forge documents and therefore it may not be as helpful as assumed.

Recommendations

There are two areas that warrant private and governmental attention. The first area is equipment technology. The number and diversity of stakeholders present impediments to coordinating technological advances. At the national level, there is a general lack of focus on long-term research, development and fielding. This is a severe shortfall in our current maritime security. Due to the various types, sizes, and functionality of and diversity in local economies, it may not be feasible to create a nation-wide priority list of prevention and detection equipment and allocate funding based on the priority list. Better security does not require spending more. The second area is developing international partnerships. Tying maritime security into the global community could also be effective. The world is globally connected and therefore so is maritime security. The feasibility of creating strategic initiatives within the international community and with foreign governments to construct maritime security equipment should be explored.

Further Study

This study recognizes current doctrine, application, funding, and the relationship among all stakeholders. The creation of Northern Command (NORTHCOM) undoubtedly helped in obtaining actionable intelligence and early warning. However, it is unclear if the problem is fixed. Various intelligence systems and bureaucracies exist. Future research should examine whether convoluted processes, information access controls, or legal constraints hinder or prevent dissemination or situational awareness.

Summary and Conclusion

President George W. Bush made it clear, "the terrorist enemy that we face is highly determined, patient, and adaptive. In confronting this, protecting our critical infrastructures and key assets represents an enormous challenge. We must remain united in our resolve, tenacious in our approach, and harmonious in our actions to overcome this challenge and secure the foundations of our Nation and way of life," (TWH 2003). This thesis suggests that all levels of government do have marginally adequate prevention measures in place to protect our seaports and key assets. Doctrine at all levels, coordination among all stakeholders, basic funding and protection measures exist. There is not enough information to answer the follow up question on whether safeguards help prevent CW/BW attacks. The GAO should continue conducting oversight of all agencies ensuring they are compliant with doctrine, policies and plans. Analysis of two ports unveiled that each implemented strategic plans at the local level and address coordination and communication with the private sector as well as other local stakeholders. A comparison matrix demonstrated that although both ports have made progress, continued

work in protecting the maritime domain security is needed. Using one system for communicating protection levels, funding, and threat analysis is vital to efficiency and common understanding. Additionally, screening and scanning should occur at port of origin if the United States is to maximize threat mitigation. Two recommended initiatives should further the maritime security goal. The first is linking R&D to a national priority list. The second is developing and working with international partners. The Obama administration's stimulus package proposal includes funding for ninety ports as of February 4, 2009. However, it is unclear if funding will address both airports and seaports, or if it will be approved by Congress.

GLOSSARY

Assessment. The evaluation and interpretation of measurements and other information to provide a basis for decision-making. (DHS 2007).

Biological agent. (DOD) A microorganism that causes disease in personnel, plants, or animals or causes the deterioration of materiel. (DHS 2007).

Biological operation. (DOD) Employment of biological agents to produce casualties in personnel or animals and damage to plants. (DHS 2007).

Biological Warfare (BW). A clandestine release of aerosols of weaponized deadly contagious disease such as smallpox, plague-infecting thousands to millions, killing 30%. (Department of Army 2004).

Biological weapons. Weapons designed to release a biological agent. Biological weapons can take many forms, such as a missile warhead or bomb. Biological weapons include any organism (such as bacteria, viruses, or fungi) or toxin found in nature that can be used to kill or injure people. (Toxins are poisonous compounds produced by organisms.) (Department of Army 2004).

Chemical agent. (DOD) Any toxic chemical substance which is intended to kill, seriously injure, or incapacitate personnel through its physiological effects. The term excludes riot control agents, herbicides, and substances generating smoke and flames. (Department of Army 2004).

Chemical Warfare (CW). (DOD) All aspects involving the employment of lethal and incapacitating munitions/agents and the warning and protective measures associated with such offensive operations. Since riot control agents and herbicides are not considered chemical warfare agents, those two items will be referred to separately or under the broader term "chemical," which will be used to include all types of chemical munitions/agents collectively. (Department of Army 2004).

Command. The act of directing, ordering, or controlling by virtue of explicit statutory, regulatory, or delegated authority (DHS 2007).

Communications. Process of transmission of information though verbal, written, or symbolic means (DHS 2007).

Critical Infrastructure. Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (DHS 2007).

Doctrine. (DOD) Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application (NATO) Fundamental principles by which the military forces guide their actions in support of objectives. It is authoritative but requires judgment in application (DHS 2007).

Emergency. Any incident (s) whether natural or manmade, that requires responsive action to protect life or property; any occasion or instance for which Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States (DHS 2007).

Evacuation. Organized, phased, and supervised withdrawal, dispersal, or removal of civilians from dangerous or potentially dangerous areas, and their reception and care in safe areas (DHS 2007).

Enemy. Any organization to include nation-states, terrorists, transnational criminals and pirates that views the United States as an adversary and is not limited to nation-states, terrorists, and transnational criminals and pirates, dispersed terrorist networks (DHS 2007).

Hazard. Something that is potentially dangerous or harmful, often the root cause of an unwanted outcome (DHS 2007).

Incident. An actual or potential emergency or all-hazards event or occurrence that range from natural or manmade to terrorist attacks, which requires a response to protect life or property (DHS 2007).

Incident Management. How incidents are managed across all homeland security activities, including prevention, protection, and response and recovery (DHS 2007).

Initial Response. Resources initially committed to an incident (DHS 2007).

Local Government. A county, municipality, city, town, township, local public authority, council of governments, regional or interstate government entity, an Indian tribe or authorized tribal entity (DHS 2007).

Maritime Domain. All areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean or other navigable waterways, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances (DHS 2007).

Nongovernmental Organization (NGO). An entity with an association that is based on interests of its members, individuals, or institutions. A government does not

create it, but it may work cooperatively with a government. Such organizations serve a public purpose, not a private benefit (DHS 2007).

Preparedness. A continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination during incident response (DHS 2007).

Prevention. Actions to avoid an incident or to intervene to stop an incident from occurring; involves actins to protect lives and property, applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations, heightened inspections, improved surveillance and security operations, investigations to determine the full nature and source of the threat (DHS 2007).

Port. Any place at which ships may discharge or receive their cargo, which is accessible on the seacoast (DHS 2007).

Private Sector. Organizations and entities that are not part of any governmental structure and include for-profit and not-for-profit organizations, formal and informal structures, commerce, and industry (DHS 2007).

Response. Activities that address the short-term, direct effects of an incident and includes immediate actions to save lives, protect property and the environment, and meet basic human needs Response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of threat (DHS 2007).

Stakeholders. Federal agencies to include executive agencies departments and government corporations, local agencies (DHS 2007).

Standard Operating Procedure (SOP). Complete reference document or an operations manual that provides the purpose, authorities, duration, and details for the preferred method of performing a single function or a number of interrelated functions in a uniform manor (DHS 2007).

Transportation security incident. A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area (DHS 2007).

Weapons of mass destruction/effect (WMD/E). For this thesis it describes chemical or biological agents or weapons and effects, terrorist attack to achieve mass effect in terms of mass casualties, destruction of critical infrastructure, economic losses, and disruption of daily life nationwide (DHS 2007).

REFERENCE LIST

Abt, Clark C., William Rhodes, Rocco Casagrande, and Gary Gaumer. *Executive Summary: The Economic Impacts of Bioterrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability.* Massachusetts: Abt Associates Inc., 2003.

Australian Government. "International Ship Code and Port facility Security Code (ISPS Code)." *IMO Circulars/Guidelines on Maritime Security* (2008). http://www.infrastructure.gov.au/transport/security/maritime/isps/index.aspx (accessed June 2, 2008).

AVANTE International Technology, Inc. *Secure Cargo Container and Supply Chain Management Based on Real-Time End-to-End Visibility and Intrusion Monitoring*. (2008). http://www.avantetech.com/whitepapers/white-papers-and-reports-on-rfid/?print=true&global (accessed June 21, 2008).

Barnett, Thomas P.M. "To Make Sea Traffic Transparent." *Washington Times*, September 30, 2008.

Blair, Dennis, and Kenneth Lieberthal. "Smooth Sailing: The World's Shipping Lanes are Safe." *Foreign Affairs* (2007). http://www.foreignaffairs.org/20070501 facomments86302/dennis-blair-kenneth-lieberthal/ (accessed November 5, 2007).

Byman, Daniel. "Brookings Institute." *Homeland Insecurities: Six years after 9/11 We're Still not Thinking Strategically*. http://www.brookings.edu/articles/2007/ 0911defense_byman.aspx?p=1 (accessed June 4, 2008).

Bouchard, Joseph F. "Center for American Progress." *New Strategies to Protect America: Safer Ports for a more Secure Economy* (2005). www.americanprogress.org/issues/2005/06/b815195.html (accessed June 21, 2008).

The Cal Trade. "Security Slack at Ports of Los Angeles, Long Beach." *The CalTrade Report* (2004). http://www.caltradereport.com/eWebObjects/print-version.cgi? dynamic (accessed June 11, 2008).

Cambridge Systematics, Inc. *Port of Miami Freight Access Study Final Report* (2007). http://www.miamidade.gov/mpo/docs/MPO_port_freight_access_200702_final.pdf (accessed June 12, 2008).

Candiotti, Susan, and Patrick Oppmann. "Port of Miami is Safe Officials say After Scare." *Cnn.com* (2007). http://edition.cnn.com/2007/US/01/07/miami.port (accessed June 28,2008).

Carafano, James J. "Homeland Security Dollars and Sense #2: Misplaced Maritime Priorities." *Heritage Foundation* (2005). http://www.heritage.org/Research/HomelandSecurity/wm648.cfm?renderforprint=1 (accessed November 5, 2007).

———. "Port Security and Foreign-Owned Maritime Infrastructure." *Heritage Foundation* (2006). http://www.heritage.org/Research/HomelandSecurity/tst030606a.cfm?renderforprint=1 (accessed November 5, 2007).

Carafano, James J., and Alane Kochems, ed. *Making the Sea Safer: A National Agenda for Maritime Security and Counterterrorism.* Washington, DC: Heritage Foundation, 2005.

CNN.com. "U.S. Ports vulnerable to Terrorists, Probe Finds", *CNN.com/US*, May27, 2008. http://edition.cnn.com/2008/US/05/27/port.security.ap/index.html (accessed May 27, 2008).

Cohen, Stephen. *Economic Impact of a West Coast Dock Shutdown* (2002). http://bre.berkeley.edu/publications/ships%202002%20final.pdf (accessed June 4, 2008).

Cornford, Phillip, and Sarah Crichton. "The Ships that Died of Shame." *Fairfax Digital* (2003). http://www.smh.com.au/articles/2003/01/13/1041990234498.html (accessed June 21, 2008).

Council for Excellence in Government. *Are we Ready? Introducing the Public Readiness Index: A Survey Based Tool to Measure the Preparedness of Individuals, Families and Communities* (2006). www.whatsyourrq.org/docs/PRI_report.pdf (accessed June 21, 2008).

Department of the Army. Field Manual 1-02 (MCRP 5-12A), *Operational Terms, and Graphics*. Washington, DC: Government Printing Office, 2004.

Department of Defense. *1997 CRPC Report to Congress – DOD Counterproliferation Program.* Washington, DC: Government Printing Office, 1997.

———. *National Military Strategy to Combat Weapons of Mass Destruction.* Washington, DC: Government Printing Office, 2006.

Department of Energy, Energy Information Administration. *The Maritime Transportation Security Act of 2002 (2002).* http://www.eia.doe.gove/oil_gas/analysis_publications/ngmajorleg/mtransport.htm (accessed June 2, 2008).

DHS. "Bureau of Customs and Border Protection – Importer Security Filing and Additional Carrier Requirements." *Federal Register.* Washington, DC: Government Printing Office, 2008.

———. *Domestic Outreach Plan*. Washington, DC: Government Printing Office, 2003.

———. *Fact Sheet: Maritime Security Requirements*. Washington, DC: Government Printing Office, 2003.

———. *Fact Sheet: Security and Prosperity Partnership.* Washington, DC: Government Printing Office, 2005.

———. *FEMA 501 - National Incident Management System*. Washington, DC: Government Printing Office, 2007.

———. *Homeland Security Presidential Directive: Homeland Security Advisory System (2007).* http://www.dhs.gov/xabout/laws/gc_1214508631313.shtm (accessed September 18, 2008).

———. *National Strategy for Maritime Security Supporting Plans Announced* (2005). http://www.dhs.gov/xnews/releases/press_release_0790.shtm (accessed June 15, 2008).

———. *National Response Framework.* Washington, DC: Government Printing Office, 2008.

———. *Secure Seas, Open Ports – Keeping our waters safe, Secure and Open for Business.* Washington, DC: Government Printing Office, 2004.

Department of Transportation. Maritime Administration. *Report to Congress on the Performance of Ports and the Intermodal System.* Washington, DC: Government Printing Office, 2005.

Florida's Domestic Security Oversight Council. *Florida's Domestic Security Annual Report* (2007). http://www.fdle.state/Domestic_Security/Library/ DS%20Annual%20Report%2007.pdf (accessed June 21, 2008).

Flynn, Stephen. America the Vulnerable – How our government is failing to protect us from Terrorism. New York: HarperCollins Publishers, 2004.

———. *The Edge of Disaster*. New York: Random House, 2007.

Helin, Kurt. "Five Years Later: Security Protects Against Attack." *Grunion Gazette Newspapers* (2006). http://www.gazettes.com/portsecurty09072006.html (accessed June 11, 2008).

KABC-TV/DT. "Security Upgrade for the Port of Long Beach." *Local News: KABC-TV/DT* (2007). http://abclocal.go.com/kabc/story?section=news/ local&id=5178606 (accessed June 11, 2008).

Kochems, Alane. "GreenLane Maritime Cargo Security Act: A Good First Attempt." *Heritage Foundation* (2006). http://www.heritage.org/research/homelanddefense/em989.cfm (accessed June 21, 2008).

———. "Taking a Global Approach to Maritime Trade Security." *Heritage Foundation* (2005). http://www.heritage.org/research/homelanddefense/em980.cfm (accessed November 5, 2007).

Kochems, Alane, and James J. Caragano. "Complete Cargo Inspection and Port Security Grants Do Not Promote Homeland Security." *Heritage Foundation* (2006). http://www.heritage.org/research/homelanddefense/em998.cfm (accessed June 12, 2008).

Korb, Lawrence J. "Six Steps to a Safer America." *Center for American Progress* (2004). http://www.americanprogress.org/issues/2004/01/b24939.html (accessed June 21, 2008).

Miami-Dade County. *Homeland Security Briefing Book 2004-2005* (2005). http://www.miamidade.gov/oem/library/homeland/Homeland-Security-Briefing-Book.pdf (accessed June 21, 2008).

Maritime Transport Committee. "Organization for Economic Co-operation and Development." *Security in Maritime Transport: Risk Factors and Economic Impact*. https://www.wecd.org/dataoecd/19/61/18521672.pdf (accessed May 27, 2008).

Miami-Dade Community College. "TV Students Participate in Domestic Preparedness Exercise." *School of Entertainment Technologies Newsletter* (2002). http://www.mdc.edu/sedt/fc/fc20025.pdf (accessed June 21, 2008).

National Commission on the Terrorist Attacks Upon the United States. *The 9/11 Commission Report.* New York: W.W. Norton and Company, 2004

Neyman, Julia. "Miami-Dade Trade Study Shows Growth in Jobs and Value Added." *South Florida Business Journal* (2008). http://www.bizjournals.com/southflorida/stories/2008/01/21/story8.html?t=printable (accessed June 12, 2008).

O'Brian, Kevin A., and Maarten Van de Voort. *Sea-curity: Improving the Security of the Global Sea-Container Shipping System*. Santa Monica, CA: RAND, 2003.

O'Brian, Thomas, and Allyson Clark. "Port Security: Guarding America's Front Door." *Ninth Annual CITT State of the Trade and Transportation Industry Town Hall Meeting*. http://www.metrans.org/documents/WhitePaper2-06-07.pdf (accessed January 8, 2009).

O'Hanlon Michael E. "Beyond Missile Defense: Countering Terrorism and Weapons of Mass Destruction." *Brookings Institute* (2008). http://www.brookings.edu/papers/2001/08defense_ohanlon.aspx?p=1 (accessed June 4, 2008).

———. "Cargo Security" *Brookings Institute* (2003). http://www.brookings.edu/testimony/2003/0320defense_ohanlon.aspx?p=1 (accessed June 4, 2008).

———. "Port Deal Raises Serious Concerns." *Brookings Institute* (2006). http://www.brookings.edu/opinions/2006/0302homelandsecurity.aspx?p=1 (accessed June 4, 2008).

———. "Protecting the American Homeland: Governor Ridge's Unfinished Work." *Brookings Institute* (2002). http://www.brookings.edu/articles/2002/summer_defense_ohanlon.aspx?p=1 (accessed June 4, 2008).

O'Rourke, Ronald. "Homeland Security: Coast Guard Operations – Background and Issues for Congress." *Congressional Research Service* (2006). http://www.fas.org/sgp/crs/homesec/RS21125.pdf (accessed June 21, 2008).

Pinzur, Matthew I. "Deal to Build Port Tunnel Closer to Reality." *Miami Herald* (2006). http://cache.search.yahoo-ht2.akadns.net/search/cache?ei=UTF-8&p=port+of+miami+strategy (accessed June 12, 2008).

Port of Long Beach. *2006-2016 Port of Long Beach Strategic Plan* (2006). http://www.polb.com/news/displaynews.asp?NewsID=46 (accessed June 21, 2008).

———. *Economic Impacts: Contributing to the Local, State, and National Economies* (2003). http://www.polb.com/about/overview/economies.asp (accessed June 21, 2008).

———. "Facts at a Glace, FAQs, Security Partnerships, C-TPAT, TWIC, Port Dive Team, Command and Control Center." *Port of Long Beach website* (2008). http://www.polb.com (accessed June 11, 2008).

Port of Miami. "Port Security, Cargo Gateway, and Port Statistics." Port of Miami website (2008). http://www.miamidade.gov (accessed June 12, 2008).

Port Security Council. *Seaport Security* (2006). http://www.portsecuritycoucil.us/issues/defalut.aspex (accessed June 4, 2008).

Public Law 107-295. 107th Congress. *Maritime Transportation Security Act of 2002*. Washington, DC: Government Printing Office, 2002.

RAND Corporation. "Sea Containers May be a Vehicle for Transporting Terrorism." *RAND Europe Study* (2003). http://www.rand.org/news/press.03/09.08.html (accessed June 4, 2008).

Repsher-Emery, Gail. "SAIC to Improve Cargo Gate System at Port of Miami." *Washington Technology* (2004). http://www.washingtontechnology.com/cgi-bin/udt/im.display.printable?client.id+washingtontechnology (accessed June 12, 2008)

Spencer, Jack. "The Future of the Coast Guard: View from the Top." *Heritage Foundation* (2005). http://www.heritage.org/Research/HomelandSecurity/wm818.cfm?renderforprint=1 (accessed November 5, 2007).

Tupan, Elizabeth, Steve Kadner, Ann Reisman, Bill Horak, and James Brown. "Areva Canberra." *Technical Issues and Organizational Demands for Combating WMD Proliferation.* http://www.canberra.com/literature/1072.asp (accessed May 20, 2008)

United States Customs and Border Protection. *2006-2011 Strategic Plan: Container Security Initiative*. Washington, DC: U.S. Customs and Border Protection, 2006.

United States Chamber of Commerce, National Chamber Foundation. *Trade and Transportation: A Study of North American Port and Intermodal Systems*. Washington, DC: Government Printing Office.2003.

United States General Accounting Office. GAO-02-993T: *Port Security – Nation Faces Formidable Challenges in Making New Initiatives Successful*. Washington, DC: GAO Office, 2002.

———. GAO-03-15*: Combating Terrorism – Actions Needed to Improve Force Protection for DOD Deployments through Domestic Seaports*. Washington, DC: GAO Office, 2002.

———. GAO-05-557: Container Security – A Flexible Staffing Model and Minimum Equipment Requirements would Improve Overseas Targeting and Inspecting Efforts. Washington, DC: GAO Office, 2005.

United States – State Department Website. Enhanced Border Security and Visa Entry Reform Act of 2002 – ALDAC No. 1. http://travel.state.gov/visa/laws/telegrams/telegrams_1403.html?css=print (accessed June 14, 2008)

Wave Dispersion Technologies, Inc. "Port Security, Maritime Security and Homeland Security Blog." *WhsiprWave* (2006). http://www.whisprwave.com/2006/05/wave-dispersion-technologies-wdt-small.html (accessed June 11, 2008).

The White House. Homeland Security Presidential Directive (HSPD) 3, *Homeland Security Advisory System.* Washington, DC: Government Printing Office, 2002.

———. Homeland Security Presidential Directive (HSPD) 13, *Maritime Security Strategy*. Washington, DC: Government Printing Office, 2004.

———. *United States National Security Strategy*. Washington, DC: Government Printing Office, 2002.

———. *United States National Strategy for Maritime Security*. Washington, DC: Government Printing Office, 2005.

———. *Maritime Commerce Security Plan for the National Strategy for Maritime Security.* Washington, DC: Government Printing Office, 2005.

———. *Maritime Infrastructure Recovery Plan for the National Strategy for Maritime Security*. Washington, DC: Government Printing Office, 2005.

———. National Security Presidential Directive (NSPD)-41, *Maritime Security Policy*. Washington, DC: Government Printing Office, 2004.

———. *National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security*. Washington, DC: Government Printing Office, 2005.

———. *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* Washington, DC: Government Printing Office, 2003.

———. *National Strategy to Combat Weapons of Mass Destruction.* Washington, DC: Government Printing Office, 2002.

Willis, Henry H., and David S. Ortiz, *Evaluating the Security of the Global Containerized Supply Chain*. Santa Monica, CA: RAND, 2004.

Zeichner Risk Analytics. "Zeichner Risk Assessment." *SAFE Port Act - Strategic Infrastructure Planning: The Resumption of Trade and Communication with Industry*. http://www.zra.com/index.htm (accessed June 14, 2008)

INITIAL DISTRIBUTION LIST

Combined Arms Research Library
U.S. Army Command and General Staff College
250 Gibbon Ave.
Fort Leavenworth, KS 66027-2314

Defense Technical Information Center/ OCA
8725 John K. Kingman Rd., Suite 944
Fort Belvoir, VA 22060-6218

Mr. Richard E. Berkebile
DJIMO
USACGSC
100 Stimson Avenue
Fort Leavenworth, KS 66027

Dr. Jack D. Kem
DJIMO
USACGSC
100 Stimson Avenue
Fort Leavenworth, KS 66027

Mr. Robert Walz
DJIMO
USACGSC
100 Stimson Avenue
Fort Leavenworth, KS 66027